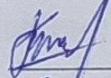


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

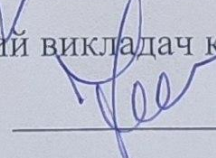
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми аналізу подій безпеки
гетерогенної мережі з використанням Splunk і Wazuh»

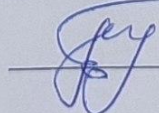
Виконала: студентка 4-го курсу групи КБ-22-2
спеціальності 125 «Кібербезпека»

 Катерина ДАНІЛЕВСЬКА

Керівник: Старший викладач кафедри КІ та КБ

 Ігор ФАЛЬКОВСЬКИЙ

Рецензент: Старший викладач кафедри КІ та КБ

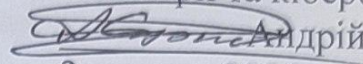
 Олександра ПОКОТИЛО

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко

2 лютого 2026 р.

ЗАВДАННЯ

на випускн у кваліфікаційну роботу бакалавра

Студентка: Данілевська Катерина Олександрівна

Тема роботи: «Проект підсистеми аналізу подій безпеки гетерогенної мережі з використанням Splunk і Wazuh»

затверджена Наказом університету від 2 лютого 2026 р. № 58/с

Термін здачі студентом закінченої роботи 9 червня 2026 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

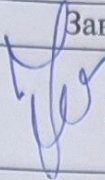
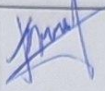
Об'єктом дослідження є процес моніторингу та аналізу подій безпеки в гетерогенній мережевій інфраструктурі.

Предметом дослідження є методи та засоби збору, обробки, індексації, аналізу й візуалізації подій безпеки з використанням Wazuh і Splunk Enterprise.

Обладнання та програмне забезпечення:

1. Oracle VM VirtualBox 7.0.14 r161095
2. Ubuntu Server 24.04 LTS
3. Ubuntu Desktop 24.04 LTS
4. Windows 10 Education 22H2
5. pfSense CE 2.8.1
6. Kali GNU/Linux Rolling 2026.1
7. Wazuh 4.14.1
8. Splunk Enterprise 10.2.3
9. Splunk Universal Forwarder 10.2.2
10. Hydra 9.6

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Старший викладач кафедри КІ та КБ Ігор ФАЛЬКОВСЬКИЙ	 14.03.2026	 14.03.2026

Студент
Керівник

Катерина ДАНІЛЕВСЬКА
Ігор ФАЛЬКОВСЬКИЙ

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	1 тиждень	Виконано
2	Аналіз предметної області та актуальності теми	2 тиждень	Виконано
3	Аналіз сучасних SIEM-систем і засобів моніторингу подій безпеки	3 тиждень	Виконано
4	Обґрунтування вибору Splunk Enterprise та Wazuh	4 тиждень	Виконано
5	Проектування структури гетерогенної мережі та підсистеми аналізу подій безпеки	5 тиждень	Виконано
6	Розгортання віртуального середовища та налаштування мережевої взаємодії	6 тиждень	Виконано
7	Встановлення та налаштування Wazuh, агентів моніторингу і Splunk Enterprise	7-8 тиждень	Виконано
8	Налаштування передавання подій Wazuh до Splunk та створення індексу подій безпеки	9 тиждень	Виконано
9	Розробка інформаційних панелей для моніторингу подій безпеки	10 тиждень	Виконано
10	Моделювання інцидентів безпеки та аналіз результатів роботи підсистеми	11 тиждень	Виконано
11	Оформлення пояснювальної записки, висновків, списку джерел і додатків	12 тиждень	Виконано

Студент

Катерина ДАНІЛЕВСЬКА

Керівник

Ігор ФАЛЬКОВСЬКИЙ

АНОТАЦІЯ

Пояснювальна записка до кваліфікаційної роботи бакалавра на тему «Проект підсистеми аналізу подій безпеки гетерогенної мережі з використанням Splunk і Wazuh» складається з 3 розділів, містить 37 рисунків, 2 таблиці, список використаних джерел із 22 найменувань, розміщений на 2 сторінках.

Метою кваліфікаційної роботи є проєктування та реалізація підсистеми аналізу подій безпеки гетерогенної мережі з використанням Splunk і Wazuh.

У роботі розглянуто актуальність моніторингу подій безпеки в гетерогенних мережах, проаналізовано особливості роботи SIEM-систем, засобів збору журналів та підходів до обробки подій безпеки. Розглянуто функціональні можливості Wazuh і Splunk Enterprise, а також визначено їх роль у побудові підсистеми аналізу подій безпеки.

У межах проєкту спроєктовано структуру гетерогенної мережі, до складу якої входять Windows та Linux хости, сервер Wazuh, сервер Splunk Enterprise і мережевий шлюз на базі pfSense. Розгорнуто та налаштовано основні компоненти підсистеми: сервер Wazuh, агенти моніторингу, сервер Splunk Enterprise та Splunk Universal Forwarder. Реалізовано передавання подій Wazuh до Splunk, створено окремий індекс для зберігання подій безпеки та налаштовано обробку JSON-повідомлень. Розроблено інформаційні панелі у Splunk для моніторингу загального стану підсистеми, аналізу мережевої активності, подій автентифікації, правил Wazuh і рівнів критичності. Наведено результати моделювання інцидентів безпеки, за результатами тестування підтверджено працездатність реалізованої підсистеми та можливість використання підсистеми для збору, аналізу й візуалізації подій безпеки в гетерогенній мережі.

Ключові слова: ПОДІЇ БЕЗПЕКИ, ГЕТЕРОГЕННА МЕРЕЖА, SIEM, WAZUH, SPLUNK, МОНІТОРИНГ, ЖУРНАЛИ ПОДІЙ, ІНФОРМАЦІЙНА БЕЗПЕКА, SPLUNK UNIVERSAL FORWARDER, DASHBOARD.

					ККІКБ.КР.Б – 125 – 04 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми аналізу подій безпеки гетерогенної мережі з використанням Splunk і Wazuh	Літ.	Арк.	Аркушів
Розроб.		Данілевська К.О.		05.06.26				
Керівник		Фальковський І.Г.		05.06.26				
Реценз.		Покотило О.А.		05.06.26				
Н. контр.		Фальковський І.Г.		05.06.26				
Затверд.		Сфіменко А.А.		06.06.26				
						ФІКТ, Гр. КБ-22-2		

ANNOTATION

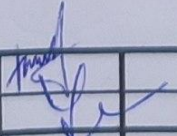
The explanatory note to the bachelor's qualification work on the topic "Project of a Security Event Analysis Subsystem for a Heterogeneous Network Using Splunk and Wazuh" consists of 3 chapters and contains 37 figures, 2 tables, and a list of references consisting of 22 sources, placed on 2 pages.

The purpose of the qualification work is to design and implement a security event analysis subsystem for a heterogeneous network using Splunk and Wazuh.

The work examines the relevance of security event monitoring in heterogeneous networks, analyzes the features of SIEM systems, log collection tools, and approaches to security event processing. The functional capabilities of Wazuh and Splunk Enterprise are considered, and their role in building a security event analysis subsystem is defined.

As part of the project, the structure of a heterogeneous network was designed, including Windows and Linux hosts, a Wazuh server, a Splunk Enterprise server, and a network gateway based on pfSense. The main components of the subsystem were deployed and configured: the Wazuh server, monitoring agents, the Splunk Enterprise server, and Splunk Universal Forwarder. The transmission of Wazuh events to Splunk was implemented, a separate index for storing security events was created, and JSON message processing was configured. Splunk dashboards were developed to monitor the general state of the subsystem, network activity, authentication events, Wazuh rules, and severity levels. The results of security incident simulation are presented. Based on the testing results, the operability of the implemented subsystem and the possibility of using it for collection, analysis, and visualization of security events in a heterogeneous network were confirmed.

Keywords: SECURITY EVENTS, HETEROGENEOUS NETWORK, SIEM, WAZUH, SPLUNK, MONITORING, EVENT LOGS, INFORMATION SECURITY, SPLUNK UNIVERSAL FORWARDER, DASHBOARD.

		Данілевська К.О.			ККИКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП	8
РОЗДІЛ 1 АНАЛІЗ СИСТЕМ МОНІТОРИНГУ ТА ОБРОБКИ ПОДІЙ БЕЗПЕКИ	10
1.1 Актуальність централізованого моніторингу подій безпеки в гетерогенних мережах.....	10
1.2 Аналіз сучасних SIEM-систем та засобів моніторингу безпеки	13
1.3 Обґрунтування архітектури підсистеми централізованого аналізу подій безпеки.....	21
1.4 Постановка технічного завдання	24
Висновки до розділу.....	26
РОЗДІЛ 2 ПРОЄКТУВАННЯ ТА РЕАЛІЗАЦІЯ ПІДСИСТЕМИ АНАЛІЗУ ПОДІЙ БЕЗПЕКИ	27
2.1 Проєктування структури гетерогенної мережі.....	27
2.2 Розгортання та налаштування компонентів підсистеми	30
2.3 Реалізація механізмів збору та аналізу подій безпеки.....	36
2.4 Реалізація системи візуалізації та моніторингу подій безпеки	40
Висновки до розділу.....	50
РОЗДІЛ 3 ТЕСТУВАННЯ ТА ОЦІНЮВАННЯ РОБОТИ ПІДСИСТЕМИ АНАЛІЗУ ПОДІЙ БЕЗПЕКИ	52
3.1 Моделювання інцидентів безпеки в гетерогенній мережі	52
3.2 Аналіз результатів виявлення подій.....	56
3.3 Оцінювання роботи інформаційних панелей після моделювання інцидентів	66
Висновки до розділу.....	73
ВИСНОВКИ.....	75
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	78
ДОДАТКИ.....	80

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				6
Змн.	Арк.	№ докум.	Підпис	Дата		

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

BSD – Berkeley Software Distribution
CSF – Cybersecurity Framework
ELK – Elasticsearch, Logstash, Kibana
FIM – File Integrity Monitoring
GDPR – General Data Protection Regulation
GPG – GNU Privacy Guard
HIDS – Host-based Intrusion Detection System
HIPAA – Health Insurance Portability and Accountability Act
IEC – International Electrotechnical Commission
IP – Internet Protocol
ISO – International Organization for Standardization
JSON – JavaScript Object Notation
MSI – Microsoft Installer
NAT – Network Address Translation
NIST – National Institute of Standards and Technology
PAM – Pluggable Authentication Modules
PCI DSS – Payment Card Industry Data Security Standard
SEM – Security Event Management
SIEM – Security Information and Event Management
SIM – Security Information Management
SOC – Security Operations Center
SPL – Search Processing Language
SSH – Secure Shell
TCP – Transmission Control Protocol
UEBA – User and Entity Behavior Analytics

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. Сучасні мережеві інфраструктури складаються з різномірних компонентів, кожен з яких формує власні журнали подій, які можуть містити важливу інформацію про стан системи, дії користувачів, спроби доступу, помилки служб або потенційно небезпечну активність.

У таких мережах проблема аналізу подій ускладнюється тим, що різні компоненти інфраструктури використовують різні формати журналів і різні механізми їх зберігання. Через це інформація про один інцидент може бути розподілена між декількома вузлами, а її ручний аналіз потребує значних витрат часу. Централізований збір і обробка таких подій дозволяє сформувати єдине джерело даних для моніторингу, пошуку, аналізу та візуалізації.

Актуальність теми полягає в необхідності побудови підсистеми, яка забезпечує об'єднання події безпеки з різних операційних систем, виконувати їх первинну обробку, передавати до централізованої платформи аналізу та подавати результати у зручному для адміністратора вигляді. Використання Wazuh і Splunk Enterprise дозволяє реалізувати такий підхід: Wazuh забезпечує збір і класифікацію подій, а Splunk – для індексації, пошуку, аналізу та побудови інформаційних панелей.

Метою кваліфікаційної роботи є проєктування та реалізація підсистеми аналізу подій безпеки гетерогенної мережі з використанням Splunk і Wazuh.

Визначена мета зумовлює такі завдання:

- дослідити особливості моніторингу подій безпеки в гетерогенних мережах.
- проаналізувати можливості Wazuh і Splunk Enterprise для збору, обробки, індексації та візуалізації подій безпеки.
- спроектувати структуру гетерогенної мережі та визначити роль її основних компонентів.
- розгорнути сервер Wazuh, сервер Splunk Enterprise, агенти моніторингу та механізм передавання подій між компонентами.
- реалізувати централізований збір і аналіз подій безпеки із Windows- та Linux-хостів.

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

- створити інформаційні панелі для моніторингу подій безпеки у Splunk.
- змоделювати інциденти безпеки та оцінити роботу реалізованої підсистеми.

Об’єктом дослідження є процес моніторингу та аналізу подій безпеки в гетерогенній мережевій інфраструктурі.

Предметом дослідження є методи та засоби збору, обробки, індексації, аналізу й візуалізації подій безпеки з використанням Wazuh і Splunk Enterprise.

У процесі виконання кваліфікаційної роботи було розроблено проєкт підсистеми аналізу подій безпеки гетерогенної мережі. Реалізована підсистема забезпечує збір подій із Windows та Linux хостів, первинну обробку повідомлень засобами Wazuh, передавання даних до Splunk Enterprise, індексацію, пошук і візуалізацію подій за допомогою інформаційних панелей моніторингу.

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 АНАЛІЗ СИСТЕМ МОНІТОРИНГУ ТА ОБРОБКИ ПОДІЙ БЕЗПЕКИ

1.1 Актуальність централізованого моніторингу подій безпеки в гетерогенних мережах

Сьогодні інформаційні системи використовуються майже в усіх сферах діяльності – від бізнесу та державного сектору до освіти й медицини. Вони забезпечують зберігання даних, підтримують комунікацію між користувачами, автоматизують робочі процеси та надають доступ до критично важливих сервісів. Через це інформаційні системи дедалі частіше стають ціллю кібератак.

За даними звіту Verizon DBIR 2025, кількість підтверджених витоків даних перевищила 12 тисяч випадків, а загальна кількість досліджених інцидентів сягнула понад 22 тисяч. Значна частина атак була пов'язана з використанням програм-вимагачів, а також із компрометацією сторонніх сервісів і постачальників. Це демонструє, що сучасні атаки стають складнішими, охоплюють одразу декілька компонентів інфраструктури та активно використовують слабкі місця різних платформ [1].

Для більшості сучасних організацій характерною є гетерогенна мережа, у якій одночасно використовуються різні операційні системи та сервіси. Кожна з цих платформ має власні механізми ведення журналів подій, власний формат логів і власні інструменти аудиту. У результаті інформація про інциденти безпеки є фрагментованою, і аналітик бачить лише окремі фрагменти загального контексту подій. Наприклад, на сервері Linux може бути зафіксована підозріла активність користувача, на Windows-станції – спроба входу з тієї ж IP-адреси, а на мережевому маршрутизаторі – аномальний трафік. Якщо ці події аналізуються окремо, вони можуть не виглядають критичними, але разом вони можуть свідчити про цілеспрямовану атаку.

Саме проблема фрагментації даних стає однією з головних причин, чому організації переходять до використання централізованого моніторингу. Коли журнали подій збираються в одному місці, з'являється можливість корелювати інциденти між різними джерелами, виявляти складні атаки та реагувати на них

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

швидше. Централізований аналіз забезпечує формування узгодженого сховища даних, де всі події зберігаються в стандартизованому форматі, доступному для пошуку та аналізу. Це значно знижує час реагування на інциденти, адже аналітик отримує не розрізнені повідомлення, а загальний контекст подій.

Актуальність централізованого моніторингу підтверджується також даними ENISA Threat Landscape 2025, де проаналізовано понад 4800 інцидентів у ЄС. Згідно зі звітом, 60% атак здійснювалися через фішинг, причому більшість кампаній використовували штучний інтелект для створення переконливих повідомлень. Програми-вимагачі залишилися найнебезпечнішою загрозою, із застосуванням подвійного та потрійного шантажу, а експлуатація нових вразливостей відбувалася протягом кількох днів після їх публікації. Це свідчить про те, що сучасні кіберзагрози швидко еволюціонують, а тому потребують систем, здатних забезпечити своєчасне виявлення та реагування [2].

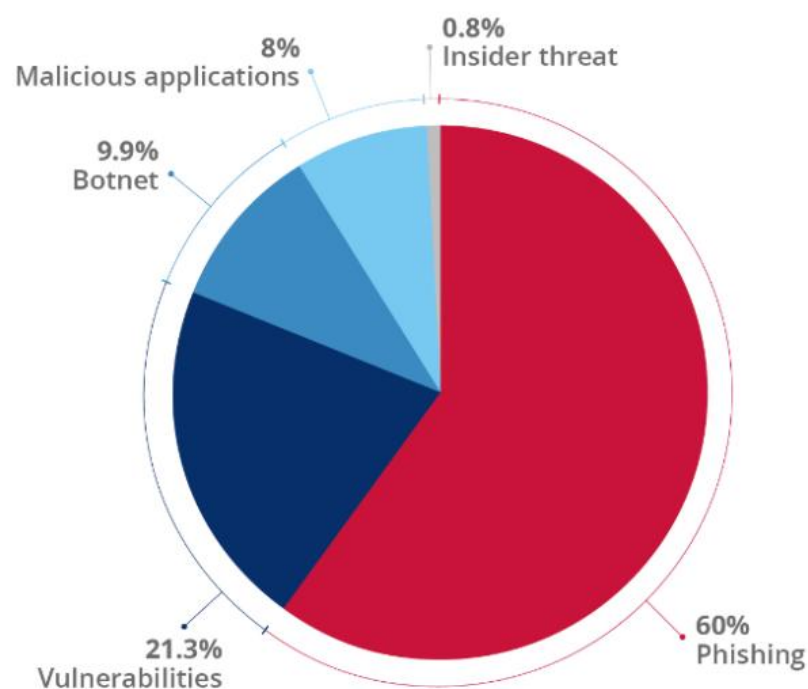


Рисунок 1.1 – Огляд загроз

Отже, актуальність централізованого моніторингу подій безпеки визначається кількома ключовими факторами:

- стрімким зростанням кіберзагроз, підтвердженим міжнародними звітами.

- складністю гетерогенних мереж, де одночасно функціонують різні платформи.
- проблемою розрізненості даних, яка ускладнює виявлення комплексних атак.
- необхідністю швидкого реагування на інциденти, що стає критично важливим у сучасних умовах.

Додатково актуальність централізованого моніторингу підсилюється вимогами міжнародних стандартів та нормативних актів. Наприклад, ISO/IEC 27001 прямо передбачає необхідність ведення журналів безпеки та їх регулярного аналізу. У розділі, що стосується контролю доступу та моніторингу, зазначається, що організація повинна забезпечувати збір і зберігання журналів подій у спосіб, який дозволяє виявляти інциденти та проводити розслідування. Без централізованого моніторингу виконати цю вимогу практично неможливо, адже журнали подій у гетерогенних мережах залишаються розкиданими між різними системами [3].

Загальний регламент захисту даних ЄС (GDPR) встановлює обов’язок організацій забезпечувати належний рівень захисту персональних даних. Це включає своєчасне виявлення та повідомлення про витоки даних. Для цього потрібні механізми централізованого моніторингу, які дозволяють швидко ідентифікувати інциденти, що стосуються персональної інформації. Таким чином, GDPR фактично зобов’язує організації мати системи, здатні здійснювати постійний контроль і аналіз подій безпеки [4].

NIST Cybersecurity Framework також визначає моніторинг як один із ключових елементів забезпечення кіберстійкості. У категорії «Detect» прямо зазначено, що організація повинна мати можливість виявляти аномалії та інциденти у реальному часі. Це можливо лише за умови централізованого збору даних із різних джерел та їх кореляції. Централізований моніторинг є не лише технологічною потребою, а й нормативною вимогою, що робить його впровадження обов’язковим для сучасних організацій [5].

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

Отримані результати свідчать, що централізований моніторинг подій безпеки в гетерогенних мережах є необхідністю, що підтверджується як статистикою міжнародних звітів, так і вимогами нормативних актів та стандартів. Він дозволяє подолати проблему розрізненості даних, забезпечує цілісне уявлення про інциденти та створює умови для своєчасного реагування на складні атаки. Отже, його впровадження є критично важливим для будь-якої сучасної організації, яка прагне зберегти кіберстійкість та захистити свої інформаційні ресурси.

1.2 Аналіз сучасних SIEM-систем та засобів моніторингу безпеки

Управління інформацією та подіями безпеки (Security Information and Event Management, SIEM) є одним із ключових напрямів сучасних систем кіберзахисту. Основне призначення SIEM-систем полягає у централізованому зборі, зберіганні, обробці та аналізі подій безпеки, що надходять із різних компонентів інформаційної інфраструктури. Такі системи дозволяють організаціям своєчасно виявляти потенційні загрози, аналізувати підозрілу активність та оперативно реагувати на інциденти безпеки до того, як вони призведуть до порушення роботи сервісів або компрометації даних.

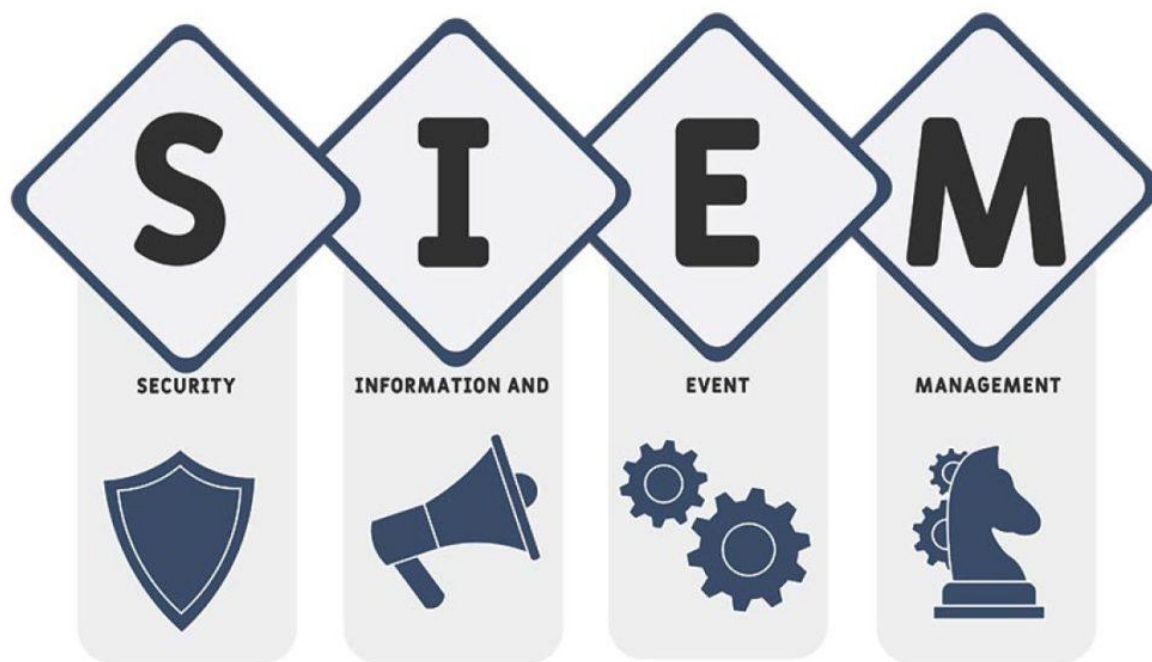


Рисунок 1.2 – Security Information and Event Management

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

Сучасна мережева інфраструктура генерує значний обсяг журналів подій. Дані надходять із серверів, робочих станцій, мережевого обладнання, систем автентифікації, міжмережевих екранів, антивірусного програмного забезпечення та інших джерел. Ручний аналіз такої кількості інформації є практично неможливим, особливо у великих організаціях. Саме тому SIEM-системи стали важливим елементом систем моніторингу безпеки, оскільки вони забезпечують автоматизований аналіз подій та допомагають виявляти аномалії у роботі мережі й користувачів.

Перші SIEM-платформи сформувалися шляхом об'єднання двох окремих напрямів: Security Information Management (SIM) та Security Event Management (SEM). Системи класу SIM були орієнтовані переважно на централізоване зберігання логів, формування звітності та підтримку аудиту безпеки. SEM-системи, своєю чергою, забезпечували моніторинг подій у режимі реального часу, аналіз журналів та генерацію сповіщень про підозрілу активність. Об'єднання цих підходів дозволило створити комплексні рішення, здатні одночасно виконувати функції збору, зберігання та оперативного аналізу подій безпеки [6].

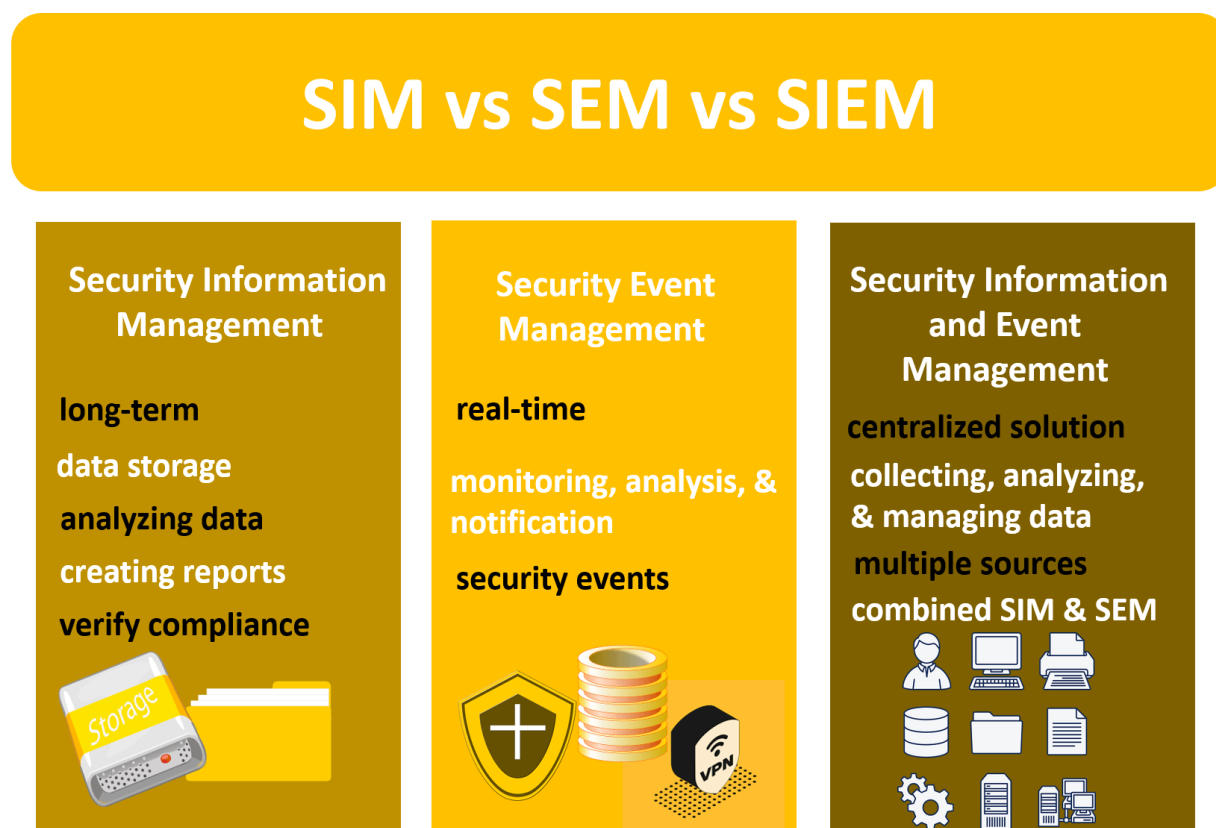


Рисунок 1.3 – Порівняння систем SIM, SEM та SIEM

Термін SIEM був офіційно запропонований аналітичною компанією Gartner у 2005 році для позначення поєднання можливостей SIM та SEM. Із цього моменту SIEM-системи почали активно розвиватися та поступово перетворилися на центральний компонент інфраструктури кібербезпеки підприємств [7].

На початкових етапах розвитку SIEM використовувалися переважно для централізованого збору логів та контролю відповідності вимогам стандартів безпеки. Проте з ускладненням кіберзагроз функціональні можливості таких систем суттєво розширилися. Сучасні SIEM-платформи підтримують механізми кореляції подій, що дозволяють встановлювати взаємозв'язки між окремими інцидентами та виявляти складні багатоступеневі атаки. Наприклад, система може зіставляти події автентифікації, мережевої активності та змін конфігурації, формуючи єдину картину потенційного інциденту безпеки.

Одним із важливих напрямів розвитку SIEM стало впровадження технологій поведінкового аналізу користувачів і систем (User and Entity Behavior Analytics, UEBA). Такі механізми дають змогу формувати типові шаблони поведінки користувачів та автоматично виявляти відхилення від нормальної активності. Це особливо важливо для виявлення внутрішніх загроз, компрометації облікових записів або атак, які не містять очевидних ознак шкідливої діяльності [7].

Крім цього, сучасні SIEM-системи активно використовують методи штучного інтелекту та машинного навчання. Їх застосування дозволяє автоматизувати частину процесів виявлення загроз, зменшити кількість хибних спрацьовувань та підвищити ефективність аналізу великих обсягів даних. Алгоритми машинного навчання можуть визначати нетипову активність, прогнозувати потенційні інциденти та допомагати аналітикам швидше реагувати на загрози [7].

Основними функціями SIEM-систем є:

- централізований збір журналів подій із різних джерел мережевої інфраструктури.
- зберігання та індексація логів для подальшого пошуку й аналізу.
- моніторинг подій безпеки в режимі реального часу.

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

- кореляція подій із різних джерел для виявлення складних атак.
- автоматичне формування сповіщень про підозрілу активність.
- виявлення аномалій у поведінці користувачів та систем.
- візуалізація даних у вигляді графіків, звітів і дашбордів.
- підтримка аудиту та контролю відповідності вимогам інформаційної безпеки.
- централізоване управління подіями безпеки.
- скорочення часу реагування на інциденти.

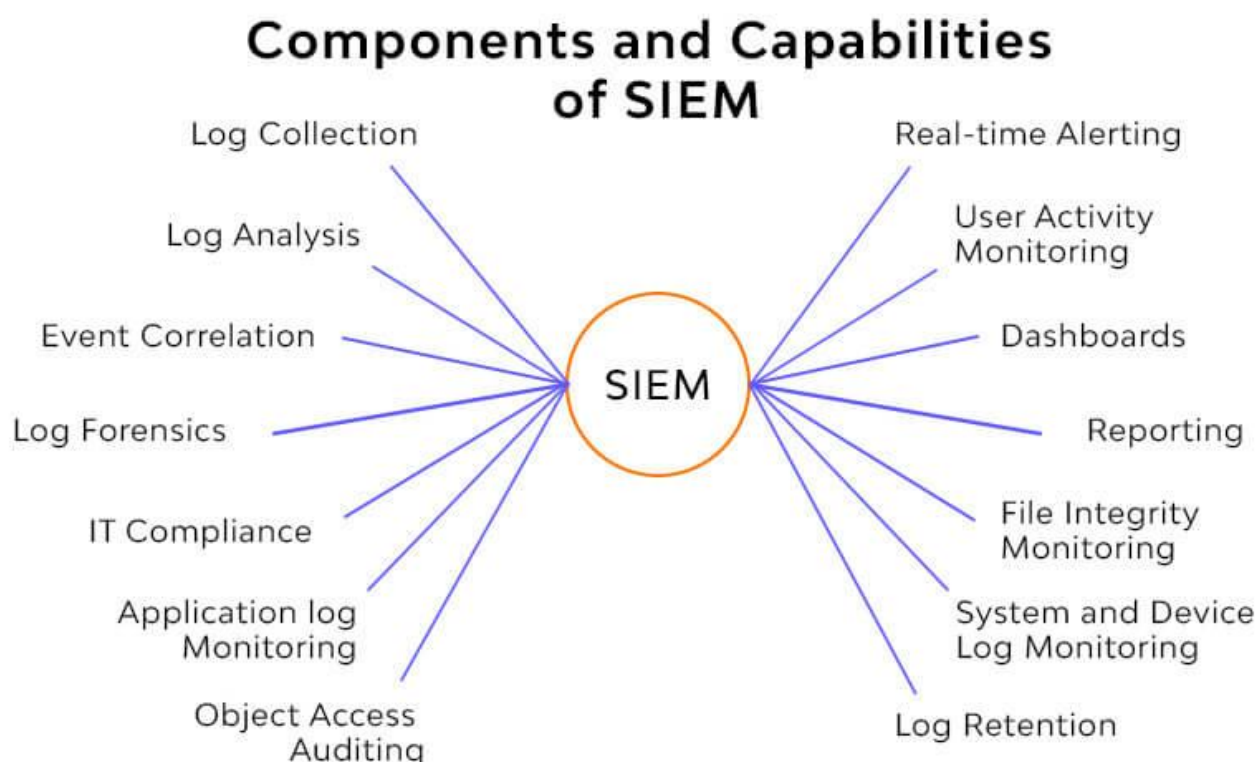


Рисунок 1.4 – Основні компоненти та функціональні можливості SIEM-систем

Ще однією важливою функцією SIEM-систем є підтримка вимог інформаційної безпеки та аудиту. Багато міжнародних стандартів і нормативних документів, зокрема GDPR, ISO/IEC 27001 та NIST, передбачають необхідність контролю подій безпеки, ведення журналів аудиту та своєчасного виявлення інцидентів. Використання SIEM дозволяє централізовано зберігати журнали подій, формувати звіти та підтверджувати дотримання вимог безпеки під час проведення перевірок.

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

На сьогодні SIEM-системи є одним із базових компонентів центрів моніторингу безпеки (Security Operations Center, SOC). Вони забезпечують централізований контроль стану інформаційної безпеки, надають інструменти для аналізу інцидентів та допомагають організаціям оперативно реагувати на сучасні кіберзагрози. Завдяки можливості інтеграції з різними платформами та засобами захисту SIEM-системи залишаються одним із найбільш ефективних рішень для забезпечення моніторингу подій безпеки у гетерогенних мережах.

Розглянуті функції є характерними для більшості сучасних SIEM-систем, однак рівень їх реалізації суттєво залежить від архітектури конкретної платформи, можливостей інтеграції, способів обробки подій та орієнтації на корпоративний або open-source сегмент. Сучасні рішення відрізняються не лише функціональними можливостями, а й підходами до збору логів, кореляції подій, автоматизації реагування та можливостей масштабування системи. Саме тому для побудови ефективної підсистеми централізованого аналізу подій безпеки доцільно розглянути найбільш поширені SIEM-рішення та засоби моніторингу безпеки, які використовуються у сучасних мережевих інфраструктурах.



Рисунок 1.5 – Огляд найбільш поширених SIEM-платформ

IBM QRadar є однією з найбільш відомих корпоративних SIEM-платформ, яка широко використовується у великих організаціях, державних установах та фінансовому секторі. Основу системи складають механізми централізованого збору та кореляції подій, що дозволяють виявляти складні багаторівневі атаки. Платформа підтримує збір логів із серверів, мережевого обладнання, баз даних,

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

систем автентифікації та хмарних сервісів із подальшою нормалізацією даних у єдиному форматі. Однією з ключових особливостей QRadar є інтеграція з сервісом IBM X-Force Threat Intelligence, який надає актуальні індикатори компрометації та інформацію про сучасні загрози. Крім цього, система підтримує аналіз мережевого трафіку, аудит подій безпеки та контроль відповідності міжнародним стандартам, зокрема PCI DSS, HIPAA та ISO/IEC 27001. До переваг QRadar можна віднести розвинуті засоби аналітики та кореляції подій, однак її використання потребує значних апаратних ресурсів і фінансових витрат [8].

ArcSight – одна з найстаріших SIEM-систем, яка тривалий час використовувалась як одна з основних платформ моніторингу безпеки у великих корпоративних середовищах. Архітектура ArcSight базується на використанні спеціалізованих конекторів, що забезпечують збір даних із різних джерел та їх подальший аналіз. Система підтримує створення складних правил кореляції подій, завдяки чому може використовуватись для виявлення комплексних атак і аномальної активності. ArcSight також має розвинуті засоби аудиту та звітності, що дозволяє організаціям забезпечувати відповідність вимогам стандартів інформаційної безпеки, зокрема ISO/IEC 27001 та NIST CSF. Перевагою системи є висока гнучкість налаштувань та підтримка великої кількості джерел подій. Водночас складність адміністрування, перевантаженість інтерфейсу та висока вартість впровадження обмежують її використання переважно великими організаціями [9].

Elastic Security є рішенням з відкритим кодом, побудованим на базі стеку Elasticsearch, Logstash та Kibana. Платформа забезпечує централізований збір, індексацію та аналіз великих обсягів даних, а також підтримує побудову інтерактивних дашбордів для моніторингу подій безпеки. Elastic Security розширює можливості ELK-стеку за рахунок функцій виявлення загроз, кореляції подій та інтеграції з агентами моніторингу. Однією з головних переваг системи є гнучкість і масштабованість, що дозволяє використовувати її як у невеликих середовищах, так і у великих розподілених інфраструктурах. Крім цього, відкритий код та активна спільнота сприяють швидкому розвитку платформи та появі великої

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

кількості інтеграцій. Недоліком Elastic Security є складність розгортання та налаштування, оскільки для ефективного використання системи необхідні знання щодо адміністрування компонентів ELK-стеку [10].

Graylog – платформа для централізованого збору та аналізу журналів подій, яка часто використовується як спрощена альтернатива ELK-стеку. Система підтримує централізований збір логів, пошук даних, фільтрацію подій та базові механізми візуалізації інформації. Graylog має відносно простий інтерфейс і не потребує складного адміністрування, що робить його популярним серед невеликих і середніх організацій. Платформа підтримує інтеграцію з різними джерелами подій та дозволяє створювати дашборди для моніторингу стану системи. Водночас можливості Graylog у сфері кореляції подій та поведінкового аналізу поступаються повноцінним корпоративним SIEM-платформам [11].

Splunk Enterprise Security є однією з найбільш поширених корпоративних платформ для централізованого аналізу подій безпеки. Система забезпечує збір і обробку великих обсягів даних, а також надає широкі можливості для пошуку, кореляції та візуалізації подій. Однією з ключових особливостей Splunk є використання власної спеціалізованої мови запитів SPL, яка дозволяє створювати складні пошукові запити, правила виявлення загроз та інтерактивні дашборди. Платформа підтримує інтеграцію з системами поведінкового аналізу користувачів (UEBA) та засобами автоматизованого реагування на інциденти (SOAR), що розширює можливості платформи у сфері моніторингу безпеки. Splunk активно використовується у великих організаціях, де необхідна обробка значних обсягів журналів подій та побудова складних сценаріїв аналізу. До основних недоліків системи належать висока вартість ліцензій та значні вимоги до апаратних ресурсів [12].

Wazuh – open-source платформа, яка поєднує функції моніторингу безпеки та виявлення вторгнень на рівні хостів. Архітектура системи базується на використанні агентів, що встановлюються на кінцеві вузли мережі, та центрального сервера для збору й аналізу подій. Wazuh підтримує моніторинг цілісності файлів, аналіз журналів подій, контроль конфігурацій, виявлення вразливостей та аудит

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

безпеки операційних систем. Платформа підтримує інтеграцію з різними системами візуалізації та аналізу даних, зокрема Elastic та Splunk, що дає змогу використовувати її як складову централізованої системи моніторингу. Перевагами Wazuh є безкоштовність, підтримка різних операційних систем та активна спільнота розробників. До недоліків належать менш розвинуті аналітичні можливості у порівнянні з великими комерційними SIEM-платформами [13].

Таблиця 1.1

Порівняльна таблиця SIEM-рішень

Система	Тип рішення	Основні переваги	Основні недоліки
IBM QRadar	Комерційна SIEM	Розвинуті засоби кореляції та аналітики	Висока вартість і значні вимоги до ресурсів
ArcSight	Комерційна SIEM	Гнучкі правила кореляції подій	Складність адміністрування
Elastic Security	Open source SIEM	Масштабованість і гнучкість	Складне налаштування
Graylog	Система аналізу логів	Простота використання	Обмежені SIEM-можливості
Splunk Enterprise Security	Комерційна SIEM	Потужні засоби пошуку та візуалізації	Висока вартість ліцензії
Wazuh	HIDS / моніторинг безпеки	Безкоштовність та підтримка різних ОС	Менш розвинуті аналітичні можливості

Проведений аналіз свідчить, що сучасні SIEM-системи суттєво відрізняються за функціональними можливостями, складністю впровадження та вартістю використання. Комерційні платформи, такі як QRadar, ArcSight та Splunk, забезпечують розвинуті засоби аналітики, кореляції подій і автоматизації реагування на інциденти, однак потребують значних фінансових та апаратних ресурсів. Open-source рішення, зокрема Elastic Security, Graylog та Wazuh, є більш доступними та гнучкішими у налаштуванні, проте можуть поступатися корпоративним системам за рівнем автоматизації та глибиною аналітики.

Для реалізації підсистеми централізованого аналізу подій безпеки в межах даної роботи було обрано інтеграцію Splunk Enterprise та Wazuh. Вибір такого підходу зумовлений необхідністю поєднання можливостей централізованої SIEM-аналітики з можливістю детального моніторингу кінцевих вузлів. Використання Splunk дозволяє реалізувати централізоване зберігання, пошук та кореляцію подій безпеки, тоді як Wazuh забезпечує моніторинг хостів, контроль цілісності файлів та збір подій із різних операційних систем.

Крім технічних можливостей, важливим фактором є поєднання комерційної SIEM-платформи з open-source компонентом. Такий підхід забезпечує гнучкість системи, знижує витрати на розгортання та водночас дозволяє зберегти широкі можливості аналізу й візуалізації даних. Особливо це важливо для гетерогенних мереж, у яких необхідно забезпечити централізований моніторинг різноманітних вузлів та джерел подій.

1.3 Обґрунтування архітектури підсистеми централізованого аналізу подій безпеки

Архітектура підсистеми централізованого аналізу подій безпеки має забезпечувати безперервний цикл обробки подій – від збору інформації на кінцевих вузлах і мережевих пристроях до централізованого аналізу, кореляції та візуалізації даних. Для гетерогенних мереж це є особливо важливим, оскільки події надходять із різних операційних систем та джерел, використовують різні формати журналів і потребують уніфікованого підходу до обробки. У таких умовах система моніторингу має забезпечувати централізований контроль усієї інфраструктури, підтримувати масштабування та дозволяти швидко виявляти інциденти безпеки.

Запропонована архітектура базується на інтеграції Splunk Enterprise та Wazuh, де кожен компонент виконує окрему функцію у процесі моніторингу та аналізу подій безпеки. Такий підхід дозволяє розподілити навантаження між компонентами системи та забезпечити поєднання моніторингу кінцевих вузлів із централізованою SIEM-аналітикою.

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				21
Змн.	Арк.	№ докум.	Підпис	Дата		

Основою архітектури є агентний підхід до збору подій. На сервери та робочі станції встановлюються агенти Wazuh, які виконують локальний моніторинг системи та передають інформацію на сервер керування. Використання агентів дозволяє здійснювати збір подій безпосередньо на рівні кінцевих вузлів, що забезпечує детальніший контроль стану системи порівняно з виключно мережевим моніторингом.

Агенти Wazuh підтримують роботу з різними операційними системами, що є важливою перевагою для гетерогенної мережевої інфраструктури. Агенти здійснюють моніторинг системних журналів, подій автентифікації, мережевої активності, змін конфігурації та стану критичних системних файлів. Крім цього, Wazuh підтримує механізми File Integrity Monitoring (FIM), які дозволяють контролювати цілісність файлів та виявляти несанкціоновані зміни у системі.

Важливою складовою архітектури є сервер Wazuh Manager, який виконує централізоване приймання та первинну обробку подій від агентів. Після отримання даних менеджер аналізує події відповідно до вбудованих правил, визначає рівень критичності подій та інцидентів та формує структуровані алерти. Такий підхід дозволяє частково виконувати фільтрацію та нормалізацію подій ще до їх передачі в центральну систему аналізу.

Події, сформовані Wazuh Manager, передаються до Splunk для подальшої індексації та аналізу. У межах запропонованої архітектури передавання даних реалізується за допомогою Splunk Universal Forwarder, який забезпечує доставку журналів подій до сервера Splunk. Використання Universal Forwarder дозволяє організувати стабільну передачу даних із мінімальним навантаженням на систему та підтримує централізоване керування потоками журналів подій.

Після надходження подій до Splunk виконується їх індексація та збереження у централізованому сховищі. Однією з головних переваг такої архітектури є можливість об'єднання подій із різних джерел у єдиному середовищі аналізу. До Splunk можуть надходити журнали подій операційних систем, дані мережевого обладнання, алерти Wazuh, журнали подій автентифікації та інші типи подій

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				22
Змн.	Арк.	№ докум.	Підпис	Дата		

безпеки. Централізоване зберігання логів значно спрощує пошук інформації та аналіз інцидентів.

Для аналізу даних у Splunk використовується мова запитів SPL (Search Processing Language), яка дозволяє виконувати пошук подій, фільтрацію даних та створення правил кореляції. Завдяки цьому система може виявляти взаємозв'язки між подіями, що надходять від різних вузлів мережі. Наприклад, невдала спроба автентифікації на Linux-сервері може бути зіставлена з подальшою підозрілою активністю на робочій станції Windows або зміною системних файлів на іншому вузлі мережі. Такий підхід дозволяє виявляти складні багатоступеневі атаки, які важко ідентифікувати при аналізі окремих журналів подій.

Окрему роль у запропонованій архітектурі відіграє централізована візуалізація даних. Splunk підтримує створення інтерактивних дашбордів, графіків та звітів, що дозволяє отримувати узагальнену інформацію про стан безпеки мережі в режимі реального часу. Використання інформаційних панелей значно спрощує моніторинг подій та дозволяє швидше реагувати на інциденти безпеки.

Запропонована архітектура також забезпечує розподіл функціонального навантаження між компонентами системи. Wazuh виконує функції моніторингу кінцевих вузлів та первинного аналізу подій, тоді як Splunk використовується як централізована SIEM-платформа для індексації, кореляції та візуалізації даних. Це дає змогу зменшити навантаження на центральний сервер аналізу та підвищити ефективність обробки подій безпеки.

Ще однією перевагою обраної архітектури є її масштабованість. У разі збільшення кількості вузлів мережі до системи можна додати нові агенти Wazuh без суттєвої зміни загальної структури підсистеми. Splunk, своєю чергою, підтримує масштабування компонентів індексації та обробки даних, що дозволяє працювати зі значними обсягами журналів подій.

Важливим фактором також є економічна доцільність використання такої архітектури. Wazuh є відкритим рішенням і не потребує придбання ліцензій для використання агентів або сервера моніторингу, що дає змогу зменшити загальну вартість впровадження системи. Використання Wazuh для попереднього аналізу та

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

структурування подій також дозволяє зменшити кількість необроблених даних, які надходять до Splunk, що є важливим з урахуванням ліцензійної моделі Splunk, що заснована на обсязі індексованих даних.

Запропонована архітектура відповідає сучасним вимогам до систем централізованого моніторингу безпеки та підтримує реалізацію основних функцій SIEM-систем: централізований збір логів, кореляцію подій, моніторинг інцидентів та аудит подій безпеки. Це дозволяє використовувати підсистему як для оперативного моніторингу мережі, так і для проведення аналізу інцидентів та формування звітності.

Узагальнюючи наведене, архітектура підсистеми централізованого аналізу подій безпеки на основі інтеграції Splunk та Wazuh забезпечує комплексний підхід до моніторингу гетерогенної мережі. Використання агентного збору подій, централізованого аналізу та механізмів кореляції дозволяє підвищити ефективність виявлення загроз, спростити аналіз подій безпеки та забезпечити централізований контроль стану мережевої інфраструктури.

1.4 Постановка технічного завдання

Метою даної роботи є розробка підсистеми аналізу подій безпеки для гетерогенної мережі з використанням Splunk Enterprise та Wazuh. Підсистема повинна забезпечувати збір, зберігання, аналіз та візуалізацію подій безпеки, що надходять із різних компонентів мережевої інфраструктури, а також надавати можливість оперативного виявлення інцидентів і контролю стану кінцевих вузлів.

Необхідність розробки такої підсистеми обумовлена зростанням кількості кіберзагроз, складністю сучасних гетерогенних мереж та потребою у централізованому контролі подій безпеки. У мережах, де одночасно використовуються різні операційні системи та сервіси, події безпеки генеруються в різних форматах і зберігаються на різних вузлах, що значно ускладнює процес моніторингу та аналізу інцидентів. Тому система повинна забезпечувати уніфікований підхід до збору та обробки журналів подій у межах єдиного середовища.

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

Основним призначенням підсистеми є забезпечення моніторингу подій безпеки та підвищення ефективності виявлення потенційних загроз у мережевій інфраструктурі. Підсистема повинна об'єднувати функції збору логів, моніторингу кінцевих вузлів, аналізу подій та візуалізації інформації, що дозволить спростити процес контролю стану мережі та реагування на інциденти безпеки.

У межах реалізації підсистеми необхідно забезпечити виконання таких основних завдань:

- централізований збір журналів подій із серверів та робочих станцій.
- моніторинг подій безпеки в операційних системах Windows та Linux.
- збір та аналіз системних журналів подій.
- виявлення підозрілої активності та потенційних інцидентів безпеки.
- централізоване зберігання подій безпеки.
- зіставлення та агрегацію подій із різних джерел даних
- пошук, фільтрацію, групування та агрегацію журналів подій.
- візуалізацію інформації за допомогою дашбордів та графіків.
- забезпечення можливості подальшого масштабування системи шляхом додавання нових вузлів і джерел подій.

У межах даної роботи також необхідно забезпечити інтеграцію компонентів підсистеми між собою та організувати передачу подій безпеки від агентів моніторингу до централізованого середовища аналізу. Реалізована система повинна забезпечувати можливість подальшого розширення функціоналу, додавання нових вузлів мережі та інтеграції з іншими джерелами подій безпеки.

Постановка технічного завдання визначає основні функціональні можливості, вимоги та призначення підсистеми аналізу подій безпеки, що реалізується у межах даної роботи. Запропонована система повинна забезпечити ефективний моніторинг подій безпеки в гетерогенній мережі, централізований аналіз журналів подій і підвищення рівня контролю стану мережевої інфраструктури.

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

Висновки до розділу

У першому розділі було проведено аналіз проблем моніторингу подій безпеки в гетерогенних мережах та обґрунтовано актуальність використання SIEM-систем для виявлення й аналізу інцидентів безпеки. Встановлено, що сучасні мережеві інфраструктури характеризуються використанням різних операційних систем, сервісів і форматів журналів подій, що ускладнює процес моніторингу та потребує централізованого підходу до збору й аналізу даних.

У межах розділу було проаналізовано сучасні SIEM-платформи та засоби моніторингу безпеки, зокрема IBM QRadar, ArcSight, Elastic Security, Graylog, Splunk Enterprise Security та Wazuh. Проведений аналіз засвідчив, що комерційні SIEM-системи мають розвинуті можливості кореляції подій, аналітики та автоматизації реагування на інциденти, однак характеризуються високою вартістю впровадження та значними вимогами до апаратних ресурсів. Open source рішення є більш гнучкими та доступними, проте можуть поступатися за рівнем аналітичних можливостей і автоматизації.

За результатами порівняння було обґрунтовано доцільність використання інтеграції Splunk Enterprise та Wazuh для реалізації підсистеми централізованого аналізу подій безпеки. Використання Splunk дозволяє забезпечити централізований збір, індексацію, кореляцію та візуалізацію подій безпеки, тоді як Wazuh забезпечує моніторинг кінцевих вузлів, контроль цілісності файлів та збір подій із різних операційних систем. Поєднання цих платформ дозволяє реалізувати комплексний підхід до моніторингу безпеки гетерогенної мережі.

Також у розділі було обґрунтовано архітектуру підсистеми централізованого аналізу подій безпеки. Запропонований підхід забезпечує централізований збір і аналіз журналів подій, можливість масштабування системи та можливість подальшого розширення функціоналу.

На завершення було сформульовано технічне завдання, визначено основні функції та вимоги до підсистеми моніторингу безпеки. Отримані результати формують основу для подальшого проєктування та практичної реалізації системи централізованого аналізу подій безпеки у наступних розділах роботи.

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				26
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2 ПРОЄКТУВАННЯ ТА РЕАЛІЗАЦІЯ ПІДСИСТЕМИ АНАЛІЗУ ПОДІЙ БЕЗПЕКИ

2.1 Проєктування структури гетерогенної мережі

Для реалізації підсистеми аналізу подій безпеки було сформовано гетерогенне мережеве середовище, до складу якого входять сервери моніторингу та аналізу подій, кінцеві вузли різних операційних систем та окремий вузол маршрутизації мережевого трафіку. Структура мережі побудована з урахуванням необхідності централізованого збору подій безпеки, розмежування функцій компонентів системи та взаємодії внутрішнього сегмента мережі із зовнішнім середовищем.

До складу розробленої мережі входять такі вузли:

- сервер Wazuh на базі Ubuntu Server 24.04 LTS.
- сервер Splunk Enterprise на базі Ubuntu Server 24.04 LTS.
- хост під керуванням операційної системи Windows 10 Education 22H2.
- хост під керуванням операційної системи Ubuntu Desktop 24.04 LTS.
- BSD-сервер, що виконує функції мережевого шлюзу, на базі pfSense CE 2.8.1.

Сервер Wazuh використовується як центральний вузол збору та обробки подій безпеки. Сервер Splunk Enterprise призначений для централізованого зберігання, пошуку та візуалізації подій безпеки. Windows- та Linux-хости виступають джерелами системних і мережевих подій, що надходять до підсистеми моніторингу. BSD-сервер використовується для організації мережевої взаємодії між внутрішнім сегментом мережі та зовнішнім середовищем.

Використання вузлів із різними операційними системами забезпечує формування подій безпеки різних типів та дозволяє реалізувати моніторинг гетерогенного середовища. Windows-хост формує системні події та події автентифікації Windows, тоді як Linux-хост генерує журнали SSH-підключень, системні повідомлення та мережеві події Linux.

Загальна структура мережі наведена на рисунку 2.1.

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

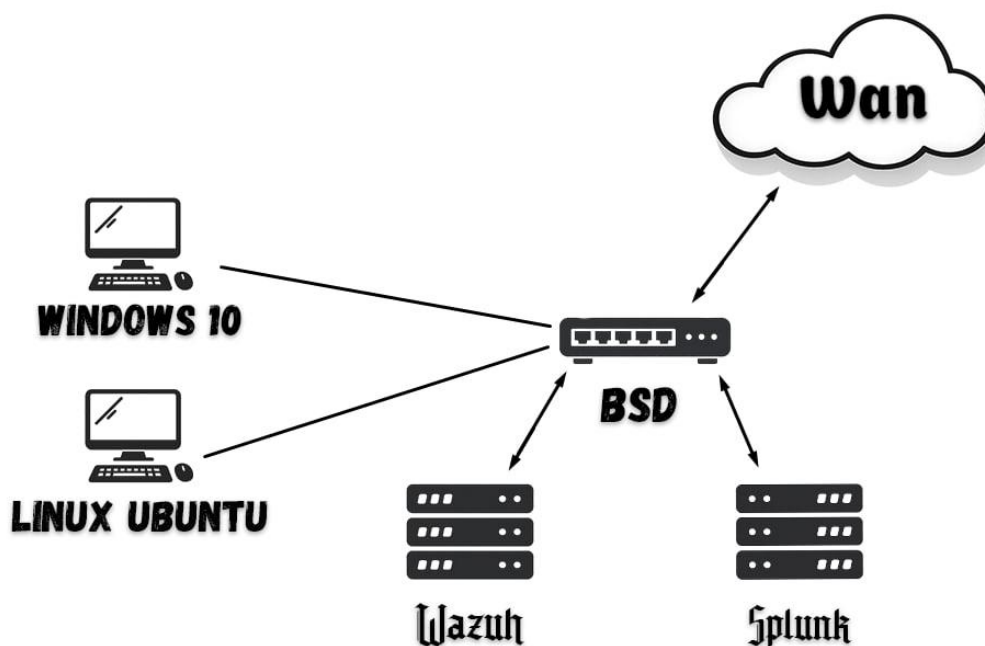


Рисунок 2.1 – Загальна структура мережі

Для забезпечення взаємодії внутрішнього сегмента мережі із зовнішнім середовищем у структурі мережі використовується окремий шлюз на базі pfSense CE 2.8.1. pfSense є дистрибутивом для маршрутизації та мережевого захисту, побудованим на базі FreeBSD – UNIX-подібної операційної системи сімейства Berkeley Software Distribution (BSD). У межах спроектованої мережі цей вузол забезпечує передавання трафіку між внутрішнім сегментом та зовнішнім середовищем, а також виконує функції централізованої маршрутизації мережевого трафіку [14].

BSD-шлюз використовує два мережеві інтерфейси. Перший інтерфейс використовується для взаємодії з локальним сегментом мережі, у межах якого функціонують сервери моніторингу та кінцеві вузли. Другий інтерфейс забезпечує доступ до зовнішнього середовища та використовується для взаємодії із зовнішніми мережевими ресурсами.

Передавання мережевого трафіку між внутрішнім і зовнішнім сегментами мережі здійснюється через BSD-шлюз, який виступає єдиною точкою маршрутизації для компонентів системи моніторингу. Це дозволяє логічно відокремити внутрішню інфраструктуру від зовнішнього середовища та забезпечує централізовану мережеву взаємодію між вузлами системи.

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

Для адресації компонентів підсистеми використовується мережа 194.42.4.0/24. Використання окремої підмережі забезпечує централізовану адресацію вузлів та спрощує адміністрування мережевої інфраструктури.

Усі компоненти підсистеми використовують статичну IP-адресацію, що забезпечує стабільну взаємодію між вузлами системи моніторингу, спрощує конфігурацію мережевих служб та забезпечує коректне функціонування компонентів підсистеми централізованого аналізу подій безпеки.

Адресний простір мережі спроектовано з урахуванням розподілу ролей між компонентами підсистеми. Сервери моніторингу та аналізу подій використовують окремі IP-адреси, що забезпечує централізовану взаємодію між компонентами системи та спрощує їх адміністрування.

Адресація вузлів та їх функціональне призначення наведені у таблиці 2.1.

Таблиця 2.1

Адресація вузлів мережі

Вузол	IP-адреса	Призначення
BSD Gateway	194.42.4.4	Маршрутизація трафіку та забезпечення взаємодії внутрішньої мережі із зовнішнім середовищем
Wazuh Server	194.42.4.10	Централізований збір та первинна обробка подій безпеки
Splunk Server	194.42.4.20	Індексація, аналіз та візуалізація подій безпеки
Windows Host	194.42.4.101	Генерація подій безпеки
Linux Host	194.42.4.102	Генерація системних та мережевих подій

Обрана схема адресації забезпечує логічне розділення компонентів підсистеми, спрощує адміністрування мережевої інфраструктури та допускає подальше розширення системи шляхом додавання нових вузлів моніторингу й агентів збору подій.

2.2 Розгортання та налаштування компонентів підсистеми

Розгортання підсистеми аналізу подій безпеки виконувалося поетапно. Спочатку було підготовлено віртуальне середовище та мережеву взаємодію між вузлами, після чого розгорнуто сервер Wazuh, підключено агенти моніторингу на кінцевих хостах, встановлено сервер Splunk Enterprise та налаштовано передавання подій між Wazuh і Splunk.

Для реалізації мережевої інфраструктури було створено окремі віртуальні машини для сервера Wazuh, сервера Splunk Enterprise, Windows-хоста, Linux-хоста та BSD-шлюзу. Внутрішній сегмент мережі було організовано у Oracle VirtualBox за допомогою мережі типу NAT Network з адресним простором 194.42.4.0/24. До цієї мережі підключено основні вузли підсистеми, що забезпечило їх взаємодію в межах локального сегмента.

BSD-шлюз було налаштовано з використанням двох мережевих підключень. Перше підключення здійснюється до NAT Network і використовується для взаємодії з внутрішнім сегментом мережі. Друге підключення виконано в режимі Bridged Adapter, завдяки чому шлюз отримує зв'язок із зовнішньою мережею через фізичний мережевий інтерфейс хостової машини. Така схема дозволяє залишити основні вузли підсистеми у відокремленому внутрішньому сегменті мережі, а вихідний трафік організувати через окремий вузол маршрутизації.

Після підготовки мережевого середовища було розгорнуто сервер Wazuh, який виконує роль центрального вузла збору та первинної обробки подій безпеки. Для встановлення серверних компонентів було підключено офіційний репозиторій Wazuh та додано GPG-ключі, що використовуються для перевірки достовірності пакетів. Після оновлення списку доступних пакетів на сервері було встановлено основні компоненти платформи: wazuh-manager, wazuh-indexer, filebeat та wazuh-dashboard [15].

Кожен із встановлених компонентів виконує окрему функцію в межах системи Wazuh. Wazuh-manager відповідає за приймання подій від агентів, їх обробку, застосування правил виявлення та формування повідомлень безпеки. Wazuh-indexer забезпечує зберігання та індексацію даних, що використовуються в

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

середовищі Wazuh для швидкого доступу до подій. Компонент filebeat використовується для передавання журналів подій між компонентами системи, а wazuh-dashboard надає вебінтерфейс для перегляду стану агентів, подій безпеки та адміністрування системи.

Після встановлення основні служби Wazuh було додано до автозапуску та запущено. Це забезпечує автоматичний запуск компонентів після перезавантаження операційної системи та їх безперервну доступність під час роботи підсистеми.

Після запуску основних служб Wazuh було виконано підключення агентів моніторингу до системи на кінцевих вузлах мережі. Для цього використовувався розділ Deploy new agent («Розгортання нового агента») у вебінтерфейсі Wazuh Dashboard. У ньому обирається тип операційної системи кінцевого вузла, задається IP-адреса сервера Wazuh та визначається група, до якої буде віднесено агент.

Рисунок 2.2 – Deploy new agent

Для Windows-хоста було обрано пакет MSI 32/64 bits, а як адресу сервера Wazuh вказано 194.42.4.10. Після вибору параметрів система автоматично сформувала команду для завантаження та встановлення агента:



Рисунок 2.3 – Команда для завантаження та встановлення агента (Windows)

Ця команда завантажує MSI-пакет агента Wazuh, виконує його встановлення у фоновому режимі та задає адресу Wazuh Manager, до якого агент має підключатися. Параметр WAZUH_MANAGER задає IP-адресу сервера Wazuh, а WAZUH_AGENT_GROUP використовується для віднесення агента до відповідної групи моніторингу.

Для Linux-хоста процес підключення виконувався аналогічно: у Wazuh Dashboard обирався відповідний тип пакета для Linux-системи, після чого система автоматично формувала команду встановлення агента із зазначенням адреси Wazuh Manager. Після встановлення службу агента запускали на кінцевому вузлі, а сам агент реєструвався на сервері Wazuh.

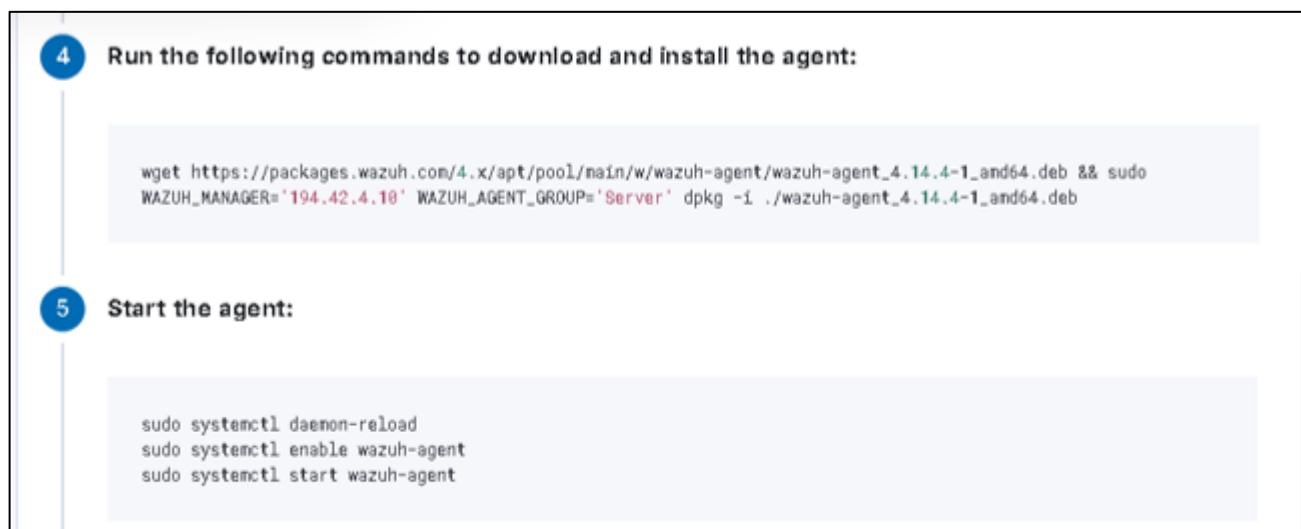


Рисунок 2.4 – Команда для завантаження та встановлення агента (Linux)

Підключення агентів дало змогу організувати збір подій із кінцевих вузлів гетерогенної мережі. Windows-агент використовується для отримання системних подій та журналів Windows Event Log, а Linux-агент – для збору системних журналів, подій автентифікації та мережевої активності Linux-хоста [16].

Після встановлення агентів їхній стан було перевірено у вебінтерфейсі Wazuh Dashboard. Відображення агентів у списку активних вузлів підтверджує їх підключення до сервера Wazuh та готовність до передавання подій безпеки.



Рисунок 2.5 – Активні агенти

Наступним етапом було розгорнуто сервер Splunk Enterprise, який у межах підсистеми використовується для централізованого приймання, індексації, пошуку та візуалізації подій безпеки. Встановлення виконувалося на окремій віртуальній машині під керуванням Ubuntu Server 24.04 LTS. Для встановлення було завантажено архів Splunk Enterprise версії 10.2.3.

Під час першого запуску Splunk було прийнято ліцензійну угоду та створено обліковий запис адміністратора, який використовується для доступу до вебінтерфейсу й подальшого керування сервером. Також було активовано автоматичний запуск Splunk після завантаження операційної системи. Це дозволяє забезпечити постійну доступність сервера без необхідності ручного запуску служби після перезавантаження [17].

Після розгортання сервера Splunk Enterprise було виконано налаштування приймання, зберігання та обробки подій Wazuh. Для цього було змінено конфігураційні файли Splunk, розміщені в каталозі /opt/splunk/etc/system/local/.

У файлі inputs.conf було активовано приймання даних на порту 9997. Цей порт використовується сервером Splunk для отримання подій від Splunk Universal Forwarder. Секція [splunktcp://9997] визначає TCP-вхід для forwarder-компонентів, а параметр disabled = 0 вказує, що приймання даних увімкнене.

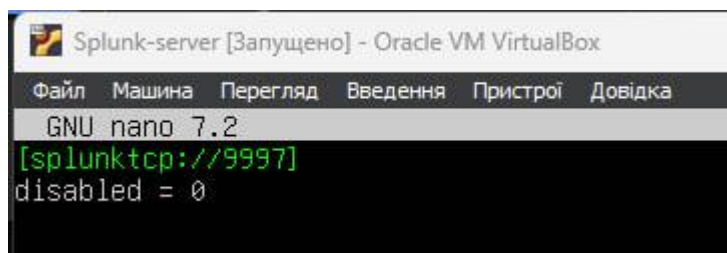


Рисунок 2.6 – Налаштування приймання даних у файлі inputs.conf

Для зберігання подій Wazuh було створено окремий індекс wazuh-alerts, параметри якого задано у файлі indexes.conf. Секція [wazuh-alerts] визначає окреме сховище для подій Wazuh. Параметр homePath задає каталог для активних даних індексу, coldPath – каталог для менш активних або архівованих даних, а thawedPath – каталог для відновлених даних. Використання окремого індексу дозволяє відокремити події Wazuh від інших журналів Splunk і спрощує подальше створення пошукових запитів та інформаційних панелей [18].

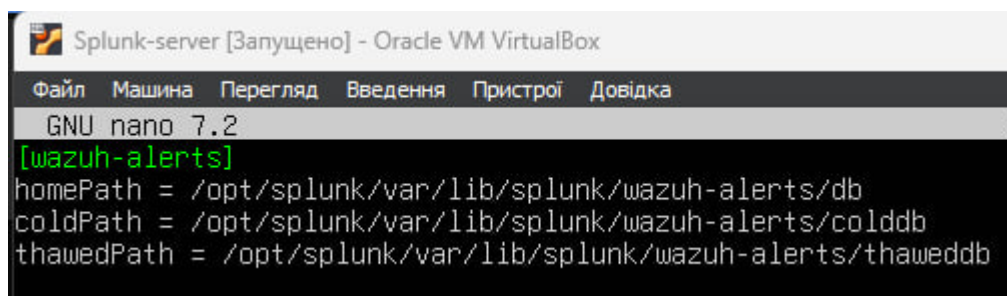


Рисунок 2.7 – Налаштування індексу wazuh-alerts у файлі indexes.conf

Для коректної обробки подій Wazuh у форматі JSON було налаштовано файл props.conf. Секція [wazuh-alerts] задає правила обробки подій відповідного sourcetype. Параметр INDEXED_EXTRactions = JSON визначає, що події мають оброблятися як JSON-структури. Це дозволяє надалі працювати з вкладеними полями подій Wazuh, зокрема agent.name, rule.level, rule.description, decoder.name та

data.srcip. Параметр KV_MODE = none вимикає додаткове автоматичне витягування key-value полів на етапі пошуку, оскільки структура подій уже обробляється як JSON. Параметр NO_BINARY_CHECK = true дозволяє обробляти файл як текстове джерело даних [19].

```

GNU nano 7.2
[wazuh-alerts]
INDEXED_EXTRactions = JSON
KV_MODE = none
NO_BINARY_CHECK = true
category = Application
pulldown_type = true

```

Рисунок 2.8 – Налаштування обробки JSON-подій у файлі props.conf

Після підготовки серверної частини Splunk було встановлено Splunk Universal Forwarder на сервері Wazuh. Його використання необхідне для передавання журналів, сформованих Wazuh, до сервера Splunk. Forwarder було встановлено саме на Wazuh Server, оскільки на цьому вузлі формується файл /var/ossec/logs/alerts/alerts.json, який містить події безпеки після первинної обробки Wazuh [20].

Для визначення сервера-отримувача було налаштовано файл outputs.conf Splunk Universal Forwarder. Секція [tcpout] задає групу передавання за замовчуванням, а секція [tcpout:default-autolb-group] містить адресу сервера Splunk. У цьому випадку forwarder передає події на сервер 194.42.4.20 через порт 9997. Отже, цей файл визначає напрямок передавання журналів від Wazuh Server до Splunk Server [21].

```

GNU nano 7.2
[tcpout]
defaultGroup = default-autolb-group

[tcpout:default-autolb-group]
server = 194.42.4.20:9997

[tcpout-server://194.42.4.20:9997]

```

Рисунок 2.9 – Налаштування сервера-отримувача у файлі outputs.conf Splunk Forwarder

Джерело подій для передавання визначено у файлі `inputs.conf` Splunk Universal Forwarder. Секція `[monitor:///var/ossec/logs/alerts/alerts.json]` вказує forwarder-у здійснювати моніторинг файлу `alerts.json`, у якому Wazuh зберігає сформовані події безпеки. Параметр `disabled = 0` активує моніторинг цього джерела. Параметр `index = wazuh-alerts` визначає індекс Splunk, до якого мають надходити події, а `sourcetype = wazuh-alerts` задає тип джерела, для якого застосовуються правила обробки з файлу `props.conf` [22].

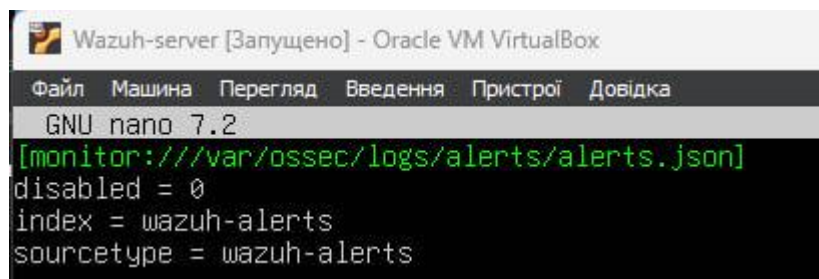


Рисунок 2.10 – Налаштування моніторингу файлу `alerts.json` у файлі `inputs.conf` Splunk Universal Forwarder

Після внесення змін до конфігураційних файлів було перезапущено Splunk Enterprise та Splunk Universal Forwarder, щоб застосувати нові параметри. У результаті сервер Splunk було підготовлено до приймання подій, а forwarder на сервері Wazuh до передавання повідомлень безпеки з файлу `alerts.json` до індексу `wazuh-alerts`.

2.3 Реалізація механізмів збору та аналізу подій безпеки

Після розгортання основних компонентів підсистеми було реалізовано механізм збору та аналізу подій безпеки. Його робота базується на послідовному передаванні подій від кінцевих вузлів до сервера Wazuh, їх первинній обробці засобами Wazuh Manager та подальшій передачі сформованих повідомлень до Splunk Enterprise.

Джерелами подій у розробленій підсистемі є Windows та Linux хости, підключені до сервера Wazuh за допомогою агентів моніторингу. На цих вузлах формуються системні журнали, події автентифікації, повідомлення про виконання адміністративних команд, SSH-підключення та інші події, що можуть свідчити про активність користувачів або зміну стану системи.

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

Агенти Wazuh виконують збір журналів на кінцевих вузлах і передають їх до Wazuh Manager. На цьому етапі події ще не є остаточними повідомленнями безпеки, оскільки потребують декодування, класифікації та зіставлення з правилами виявлення. Обробка подій на сервері Wazuh дозволяє визначити тип активності, джерело події, рівень критичності та додаткові параметри, необхідні для подальшого аналізу.

Wazuh Manager виконує первинний аналіз отриманих журналів. У процесі обробки застосовуються декодери та правила виявлення, за допомогою яких система визначає, до якого типу належить подія. Наприклад, події автентифікації можуть бути класифіковані як успішні або невдалі спроби входу, виконання команд із підвищеними привілеями або відкриття й закриття користувацьких сесій. Для кожної події формується опис, ідентифікатор правила, рівень критичності та інформація про вузол, з якого вона надійшла.

Результати обробки Wazuh зберігаються у файлі «/var/ossec/logs/alerts/alerts.json». Цей файл містить сформовані повідомлення безпеки у форматі JSON. Використання такого формату дозволяє зберігати події у структурованому вигляді та надалі використовувати окремі поля під час пошуку, фільтрації та побудови аналітичних запитів у Splunk.

```
{
  "timestamp": "2026-05-20T16:13:00.976+0000",
  "rule": {
    "level": 3,
    "description": "Software protection service scheduled successfully.",
    "id": "60642",
    "firedtimes": 4,
    "all": false,
    "groups": [
      "windows",
      "windows_application"
    ],
    "agent": {
      "id": "001",
      "name": "DESKTOP-V3EKL0Q",
      "ip": "194.42.4.101",
      "manager": {
        "name": "wazuhserver",
        "id": "79293580-279198",
        "decoder": {
          "name": "windows_eventchannel",
          "data": {
            "win": {
              "system": {
                "providerName": "Microsoft-Windows-Security-SPP",
                "providerGuid": "{E23833B0-C9-472C-ASF9-F2BDFEAF156}",
                "eventSourceName": "Software Protection Platform Service",
                "eventID": "16384",
                "version": "0",
                "level": "4",
                "task": "0",
                "opcode": "0",
                "keywords": "0x0000000000000000",
                "systemTime": "2026-05-20T16:13:06.819421200Z",
                "eventRecordID": "1674",
                "processID": "0",
                "threadID": "0",
                "channel": "Application",
                "computer": "DESKTOP-V3EKL0Q",
                "severityValue": "INFORMATION",
                "message": "\\Successfully scheduled Software Protection service for re-start at 2026-05-21T15:50:06Z. Reason: RulesEngine.\\",
                "eventdata": {
                  "data": "2026-05-21T15:50:06Z, RulesEngine",
                  "location": "EventChannel"
                }
              }
            }
          }
        },
        "timestamp": "2026-05-20T17:04:33.783+0000",
        "rule": {
          "level": 3,
          "description": "Wazuh server started.",
          "id": "502",
          "firedtimes": 1,
          "mail": false,
          "groups": [
            "ossec"
          ],
          "ci_dss": [
            "10.6.1"
          ],
          "gpg13": [
            "10.1"
          ],
          "gdnr": [
            "IV_35.7.d"
          ],
          "hipaa": [
            "164.312.b"
          ],
          "nist_800_53": [
            "AU.6"
          ],
          "tsc": [
            "CC7.2",
            "CC7.3"
          ],
          "agent": {
            "id": "000",
            "name": "wazuhserver",
            "manager": {
              "name": "wazuhserver",
              "id": "1779296673.280796",
              "full_log": "ossec: Manager started.",
              "decoder": {
                "name": "ossec",
                "location": "wazuh-monitord"
              }
            },
            "timestamp": "2026-05-20T17:10:29.729+0000",
            "rule": {
              "level": 4,
              "description": "PAM misconfiguration.",
              "id": "5553",
              "firedtimes": 1,
              "mail": false,
              "groups": [
                "pam",
                "slog"
              ],
              "pci_dss": [
            "10.6.1"
          ],
              "gpg13": [
            "4.3"
          ],
              "gdnr": [
            "IV_35.7.d"
          ],
              "hipaa": [
            "164.312.b"
          ],
              "nist_800_53": [
            "AU.6"
          ],
              "tsc": [
            "CC7.2",
            "CC7.3"
          ],
              "agent": {
                "id": "000",
                "name": "wazuhserver",
                "manager": {
                  "name": "wazuhserver",
                  "id": "1779297029.281046",
                  "full_log": "May 20 17:10:29 wazuhserver login[895]: PAM unable to dlopen(pam_lastlog.so): sr/lib/security/pam_lastlog.so: cannot open shared object file: No such file or directory",
                  "predecoder": {
                    "program_name": "login",
                    "timestamp": "May 20 17:10:29",
                    "ostname": "wazuhserver",
                    "decoder": {}
                  },
                  "location": "journalid"
                }
              }
            }
          }
        }
      }
    }
  }
}
```

Рисунок 2.11 – Фрагмент файлу alerts.json із подіями Wazuh

Типова подія Wazuh має структурований вигляд і складається з кількох основних груп полів. Група agent містить інформацію про вузол, з якого надійшла подія, зокрема ім'я агента та його ідентифікатор. Група rule описує правило Wazuh, яке спрацювало під час аналізу події. До неї входять ідентифікатор правила, рівень критичності, текстовий опис події та групи правил, до яких вона належить.

Група decoder визначає механізм декодування, який було застосовано до вхідного журналу. Наприклад, для подій SSH може використовуватися декодер

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

sshd, а для подій автентифікації – pam. Група data містить додаткові параметри події, які залежать від її типу: IP-адресу джерела, ім'я користувача, назву процесу або інші атрибути журналу. Група manager містить інформацію про сервер Wazuh, який виконав обробку події.

Така структура дозволяє зберігати повідомлення безпеки у впорядкованому вигляді та використовувати окремі поля під час подальшого аналізу в Splunk. Наприклад, поля agent.name, rule.level, rule.description, decoder.name, data.srcip та data.dstuser можуть застосовуватися для фільтрації подій, побудови таблиць, групування за рівнем критичності та створення інформаційних панелей моніторингу.

Передавання сформованих подій до Splunk реалізовано через Splunk Universal Forwarder, встановлений на сервері Wazuh. Forwarder здійснює моніторинг файлу alerts.json і передає нові записи до сервера Splunk. На стороні Splunk події потрапляють до індексу wazuh-alerts, що дозволяє відокремити їх від інших журналів і використовувати окремі пошукові запити для аналізу подій безпеки.

Після надходження до Splunk події можуть бути оброблені за допомогою SPL-запитів. Оскільки повідомлення Wazuh мають JSON-структуру, для роботи з вкладеними полями використовується команда spath, яка дозволяє звертатися до таких полів, як agent.name, rule.level, rule.description, data.srcip, data.dstuser та decoder.name.

Для базового перегляду подій було сформовано запит, який виводить основні атрибути повідомлень безпеки: час виникнення події, вузол-джерело, опис правила, рівень критичності та декодер, що обробив подію. Базове табличне подання використовується як проміжний етап між отриманням необроблених подій та побудовою аналітичних панелей. Воно дозволяє переконатися, що після передавання з Wazuh до Splunk події зберігають ключові атрибути, необхідні для подальшої фільтрації та групування. Зокрема, на цьому етапі важливо, щоб у результатах пошуку були доступні поля, пов'язані з агентом, правилом виявлення, рівнем критичності та декодером події. Саме ці атрибути надалі використовуються

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				38
Змн.	Арк.	№ докум.	Підпис	Дата		

для формування зведених показників, таблиць останніх подій і графіків розподілу за рівнями критичності.

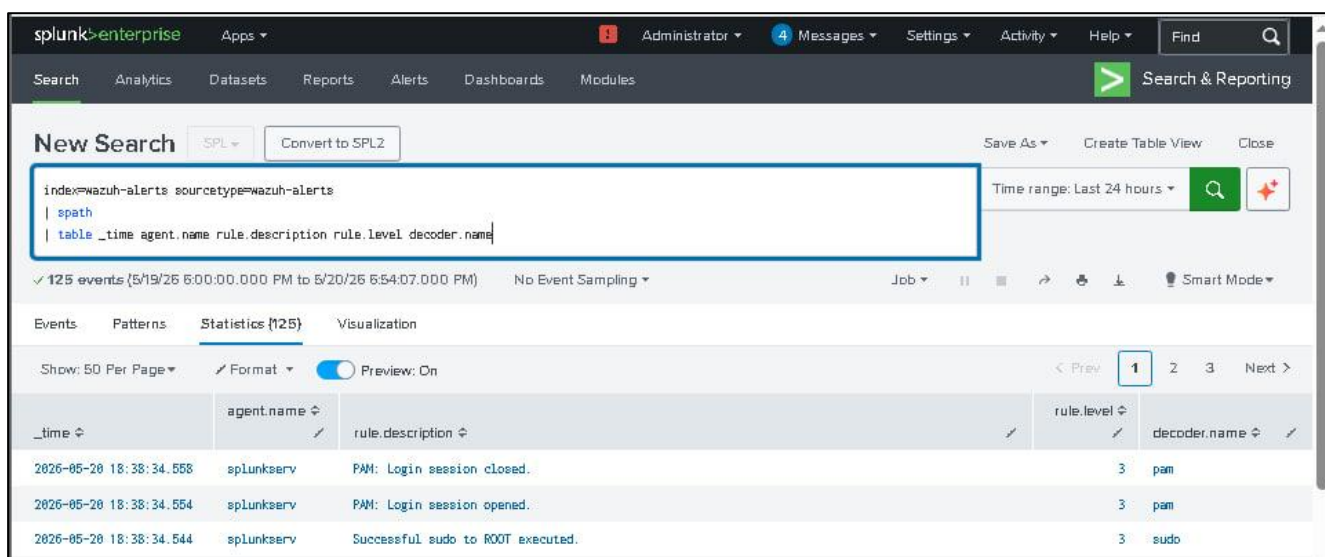


Рисунок 2.12 – Відображення основних полів подій Wazuh у Splunk

На рисунку видно, що події після індексації зберігають структуровані поля, сформовані Wazuh. Зокрема, поле `agent.name` дозволяє визначити вузол, з якого надійшла подія, `rule.description` містить опис спрацьованого правила, `rule.level` показує рівень критичності, а `decoder.name` вказує тип декодера, який був застосований до журналу. Таке подання є зручним для первинного перегляду подій і підтверджує можливість роботи з вкладеними JSON-полями у Splunk.

Для подальшого аналізу було сформовано уніфіковане табличне подання подій. Його призначення полягає в тому, щоб привести різні типи подій Wazuh до однакової структури відображення. Це важливо, оскільки не всі події містять однаковий набір атрибутів: наприклад, SSH-події можуть містити IP-адресу джерела, тоді як локальні PAM- або sudo-події можуть не мати мережових параметрів.

У запиті для такого подання використовуються команди `coalesce` та `fillnull`. Команда `coalesce` дозволяє вибрати перше доступне значення з кількох можливих полів, а `fillnull` використовується для заміни відсутніх значень службовим символом. Завдяки цьому таблиця зберігає однакову структуру навіть тоді, коли окремі поля відсутні в певному типі події. Результат такого уніфікованого подання наведено на рисунку 2.13.

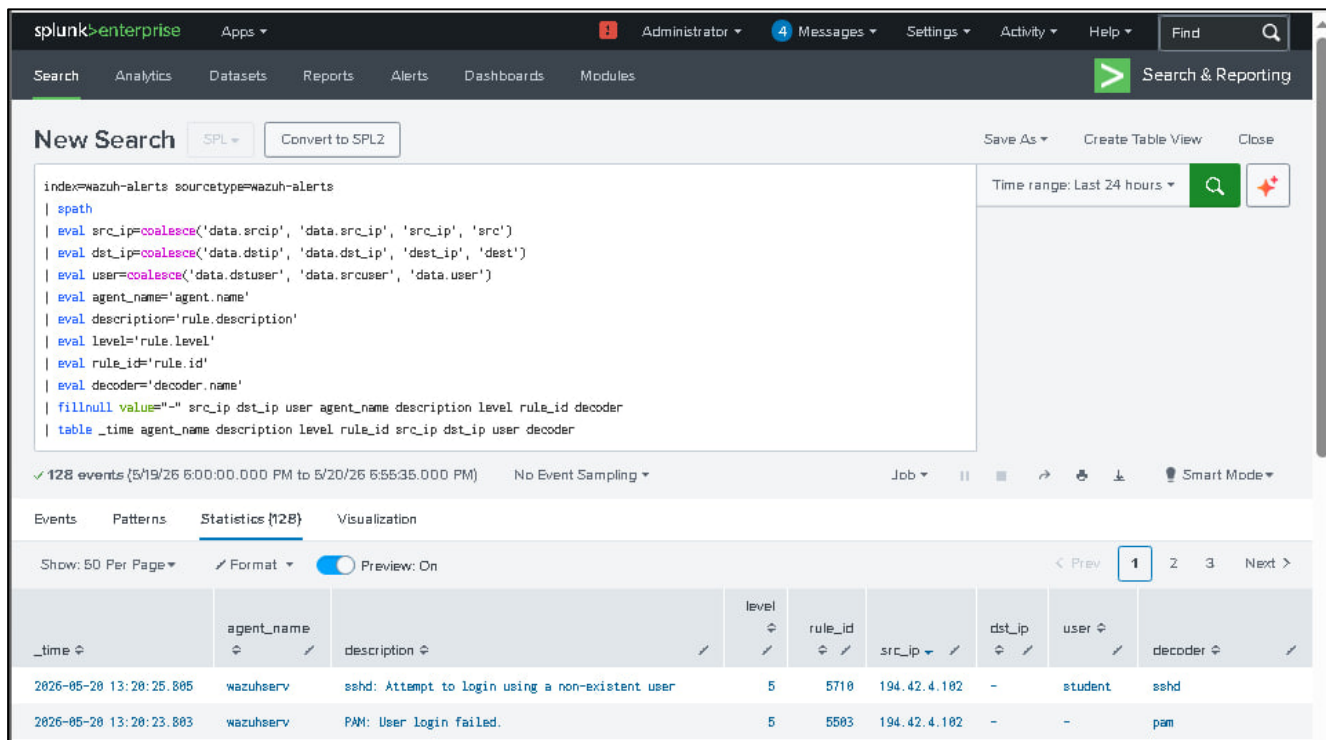


Рисунок 2.13 – Уніфіковане табличне подання подій Wazuh у Splunk

На рисунку показано приклад подій, у яких відображаються нормалізовані поля `agent_name`, `description`, `level`, `rule_id`, `src_ip`, `dst_ip`, `user` та `decoder`. Такий формат надалі використовується для побудови таблиць у дашбордах, фільтрації подій за користувачами або IP-адресами, аналізу рівнів критичності та визначення типів подій за декодерами.

Реалізований механізм забезпечує повний цикл централізованого опрацювання подій: від їх формування на кінцевих вузлах і первинного аналізу у Wazuh до індексації та подальшої аналітичної обробки у Splunk. Це створює основу для побудови інформаційних панелей, моніторингу подій автентифікації, аналізу активності користувачів і оцінювання рівнів критичності подій безпеки.

2.4 Реалізація системи візуалізації та моніторингу подій безпеки

Для забезпечення зручного аналізу подій безпеки у підсистемі було реалізовано систему інформаційних панелей у Splunk Enterprise. Візуалізація даних дозволяє подати результати збору та обробки подій у вигляді графіків, таблиць і числових показників, що спрощує моніторинг стану мережевої інфраструктури та виявлення підозрілої активності.

Основою для побудови інформаційних панелей є події, що надходять до індексу wazuh-alerts. Для їх обробки використовуються SPL-запити, які дозволяють фільтрувати події, групувати їх за вузлами, рівнями критичності, правилами Wazuh, користувачами та IP-адресами. Оскільки події Wazuh мають JSON-структуру, у запитах застосовується команда `spath`, що забезпечує доступ до вкладених полів, зокрема `agent.name`, `rule.level`, `rule.description`, `decoder.name` та `data.srcip`.

У межах реалізації системи моніторингу було створено чотири інформаційні панелі:

- Security Overview – загальний огляд стану підсистеми.
- Network Activity – моніторинг мережевої активності.
- Authentication Monitoring – аналіз подій автентифікації.
- Rule & Severity Analysis – аналіз правил Wazuh та рівнів критичності подій.

Поділ системи візуалізації на декілька дашбордів дозволяє розмежувати різні напрями аналізу подій безпеки. Замість розміщення всіх показників в одному перевантаженому екрані, кожна інформаційна панель орієнтована на окремий аспект моніторингу: загальний стан підсистеми, мережеву активність, події автентифікації або аналіз правил і рівнів критичності. Такий підхід спрощує навігацію між показниками та дозволяє швидше переходити від загальної оцінки стану системи до деталізованого аналізу конкретної категорії подій. Для загального моніторингу використовуються числові показники, графіки динаміки подій у часі, діаграми розподілу, таблиці останніх подій та панелі взаємозв'язків між джерелами даних і типами подій.

Першою інформаційною панеллю є Security Overview, призначена для загального огляду стану підсистеми аналізу подій безпеки. Вона використовується як основна панель моніторингу та дозволяє швидко оцінити кількість подій, активність вузлів, рівні критичності та останні зафіксовані повідомлення безпеки.

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				41
Змн.	Арк.	№ докум.	Підпис	Дата		

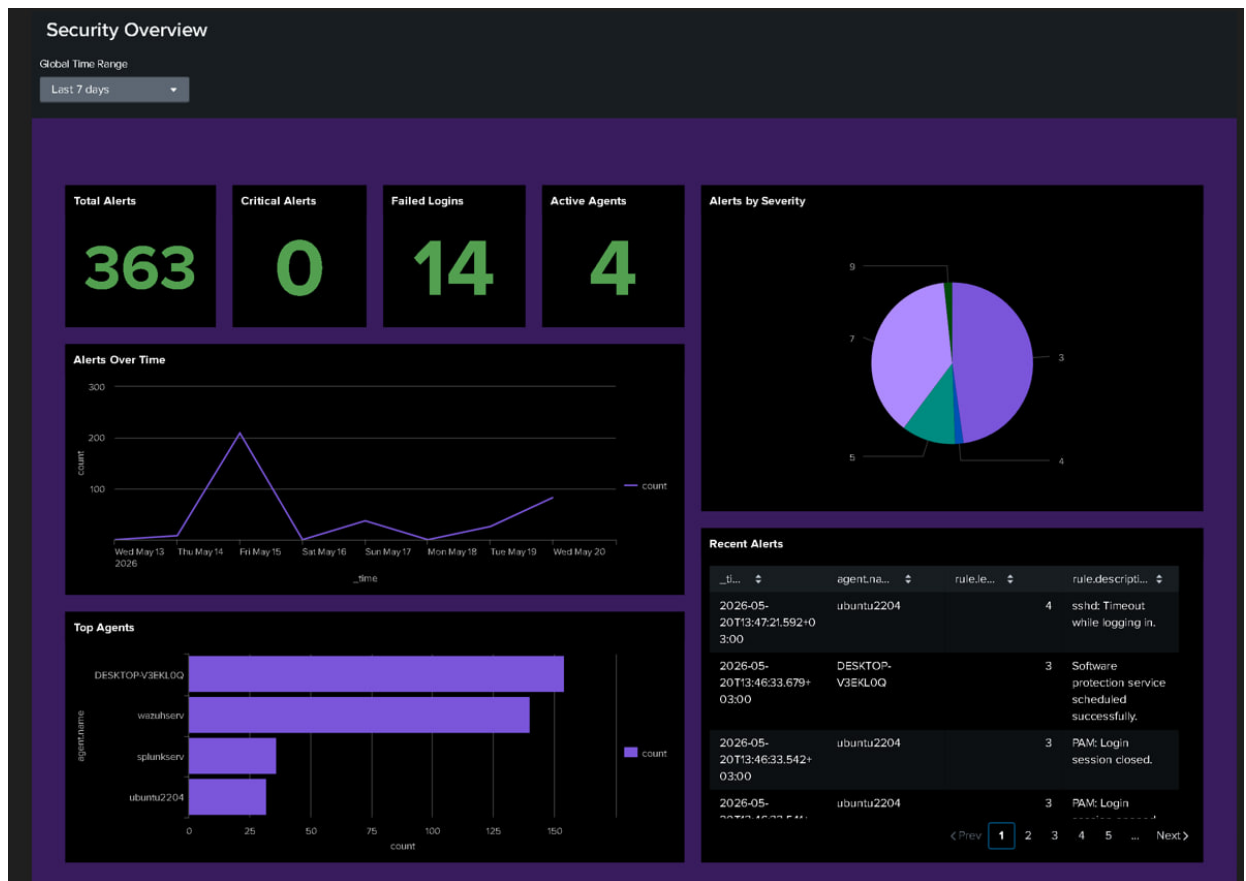


Рисунок 2.14 Security Overview

У верхній частині дашборда розміщено елемент Global Time Range, який задає часовий інтервал для всіх відображених даних. Завдяки цьому користувач може аналізувати події за останні години, добу, тиждень або інший обраний період. Єдиний часовий фільтр забезпечує узгодженість усіх елементів візуалізації, оскільки числові показники, графіки та таблиці оновлюються відповідно до одного й того самого проміжку часу.

Верхній блок дашборда містить ключові числові показники, які дають змогу швидко оцінити поточний стан підсистеми. Показник Total Alerts відображає загальну кількість подій, що надійшли до індексу wazuh-alerts за обраний період. Critical Alerts використовується для контролю наявності подій із високим рівнем критичності. У поточному стані системи цей показник дорівнює нулю, що свідчить про відсутність критичних повідомлень у вибраному часовому діапазоні. Показник Failed Logins відображає кількість невдалих спроб автентифікації, що є важливим для виявлення потенційних спроб несанкціонованого доступу. Active Agents

показує кількість вузлів, від яких надходять події безпеки, і дозволяє оцінити охоплення моніторингом компонентів мережі.

Динаміку надходження повідомлень відображає графік Alerts Over Time. Він показує зміну кількості подій у часі та дозволяє виявляти періоди підвищеної активності. Різке зростання кількості подій може свідчити про інтенсивну роботу користувачів, зміну стану системи, появу помилок або потенційно підозрілу активність. У межах загального огляду цей графік дає змогу швидко визначити часові проміжки, які потребують детальнішого аналізу.

Діаграма Alerts by Severity використовується для оцінювання розподілу подій за рівнями критичності Wazuh. Така візуалізація дозволяє визначити, які рівні подій переважають у системі, та швидко оцінити загальний рівень ризику. Якщо більшість подій належить до низьких або середніх рівнів, це може свідчити про штатну активність системи. Наявність подій високої критичності потребує подальшого аналізу в спеціалізованому дашборді, присвяченому правилам і рівням критичності.

Окремий блок Top Agents показує розподіл подій між вузлами мережі. Завдяки цьому можна визначити, які агенти генерують найбільшу кількість повідомлень за вибраний період. Такий показник є корисним для оцінювання активності окремих хостів, виявлення надмірного журналювання або визначення вузлів, які потребують додаткової уваги.

У нижній частині дашборда розміщено таблицю Recent Alerts, яка відображає останні зафіксовані події. Табличне подання містить час виникнення події, назву агента, рівень критичності та опис правила Wazuh. На відміну від зведених графіків, цей елемент дозволяє одразу перейти до перегляду конкретних повідомлень безпеки, що зручно для первинного аналізу, коли потрібно швидко зрозуміти, які саме події сформували поточні числові показники та графіки.

Отже, Security Overview виконує функцію узагальненого екрана контролю стану підсистеми. Він поєднує кількісні метрики, часову динаміку, розподіл за критичністю, активність агентів і таблицю останніх подій. Така структура дозволяє швидко оцінити загальний стан мережевого середовища, виявити аномальне

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

зростання кількості подій, перевірити наявність критичних повідомлень і визначити вузли, які є найбільш активними джерелами подій безпеки.

Дашборд Network Activity призначений для моніторингу мережевої активності та подій, у яких присутні ознаки взаємодії між вузлами мережі. На відміну від загального дашборда, цей екран зосереджений не на всіх подіях підсистеми, а на тих повідомленнях, які пов'язані з IP-адресами, мережевими підключеннями, SSH-активністю та декодерами, що характеризують мережеву або системну взаємодію.

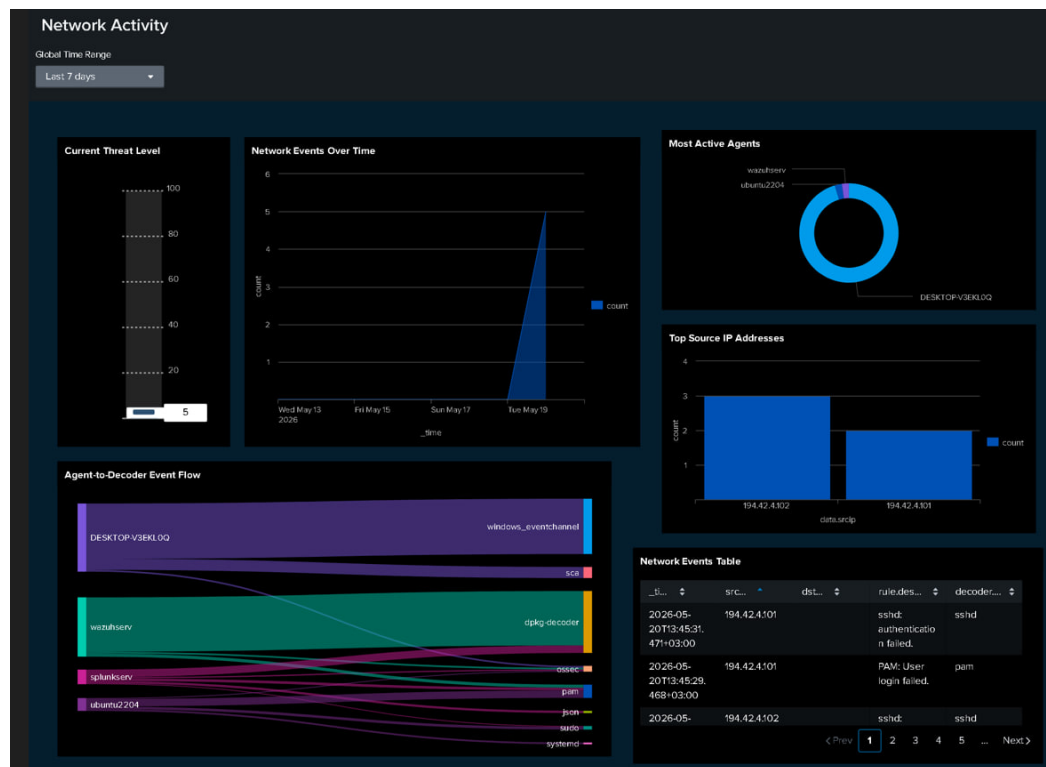


Рисунок 2.15 Network Activity

Для швидкої оцінки поточного стану використано індикатор Current Threat Level. Він відображає узагальнений рівень загрози на основі середнього рівня критичності подій. Такий елемент не замінює детальний аналіз, але дозволяє швидко оцінити загальний стан мережевої активності та звернути увагу на можливе зростання ризику.

Графік Network Events Over Time показує динаміку мережевих подій у часі. Він дозволяє визначити періоди, коли кількість мережевих повідомлень зростає, наприклад унаслідок SSH-підключень, невдалих спроб автентифікації або іншої

активності між вузлами. Така візуалізація корисна для первинного виявлення часових проміжків, які потребують подальшого аналізу.

Окремо відображається розподіл активності між агентами. Елемент Most Active Agents показує, які вузли генерують найбільшу кількість подій за вибраний часовий проміжок. Це дозволяє оцінити, які компоненти мережі є найбільш активними джерелами подій, і порівняти активність серверів та кінцевих хостів.

Діаграма Top Source IP Addresses використовується для аналізу IP-адрес, з яких надходить найбільша кількість мережевих подій. Це дозволяє відстежувати активність окремих вузлів, що ініціюють підключення або формують події з IP-атрибутами. Надалі така панель може використовуватися для виявлення підозрілих зовнішніх адрес під час моделювання атак або сканування.

Особливістю цього дашборда є візуалізація Agent-to-Decoder Event Flow, яка показує зв'язок між агентами та декодерами Wazuh. Вона дозволяє побачити, які типи подій формуються різними вузлами мережі. Наприклад, Windows-хост пов'язується з декодером windows_eventchannel, Linux-хост – із декодерами ram, sshd, sudo або systemd, а серверні компоненти можуть генерувати службові системні події. Такий підхід дає змогу не лише оцінити кількість подій, а й зрозуміти їх походження та тип обробки.

Таблиця Network Events Table використовується для детального перегляду окремих мережевих подій. У ній відображаються час події, IP-адреса джерела, IP-адреса призначення за наявності, опис правила та декодер. Табличне подання доповнює графіки й дозволяє перейти від загальної картини до аналізу конкретних повідомлень безпеки.

Таким чином, дашборд Network Activity забезпечує окремий рівень моніторингу мережевої взаємодії в межах підсистеми. Він дозволяє аналізувати часову динаміку подій, активність окремих вузлів, джерела мережевих повідомлень і зв'язок між агентами та типами декодерів Wazuh. Це робить його корисним для виявлення нетипової активності, аналізу SSH-подій та контролю взаємодії між компонентами гетерогенної мережі.

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		45

Дашборд Authentication призначений для моніторингу подій автентифікації та дій користувачів у межах гетерогенної мережі. На відміну від загального огляду, цей дашборд зосереджений саме на входах у систему, SSH-підключеннях, невдалих спробах автентифікації, sudo-активності та користувачах, які найчастіше фігурують у подіях безпеки.

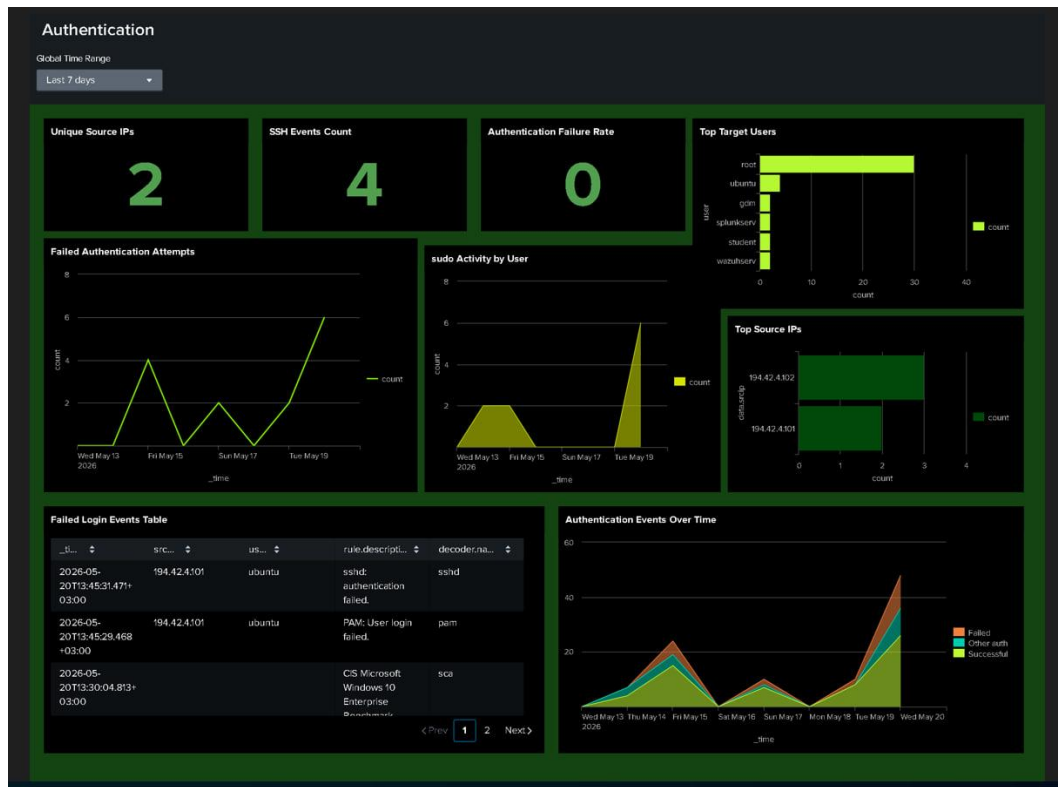


Рисунок 2.16 Authentication

У верхній частині розміщено зведені показники, які дозволяють швидко оцінити стан автентифікаційної активності за вибраний період. Unique Source IPs показує кількість унікальних IP-адрес, з яких були зафіксовані спроби підключення або події з мережевими атрибутами. SSH Events Count відображає загальну кількість SSH-подій, що дозволяє оцінити активність віддаленого доступу до Linux-вузлів. Authentication Failure Rate використовується як індикатор частки невдалих спроб автентифікації у загальному потоці подій.

Основна частина відображає динаміку подій автентифікації у часі. Графік Failed Authentication Attempts показує зміну кількості невдалих спроб входу протягом вибраного періоду. Зростання цього показника може свідчити про помилки користувачів, неправильні облікові дані або потенційні спроби несанкціонованого доступу. Окремо відображено sudo Activity by User, що

дозволяє контролювати виконання команд із підвищеними привілеями. Такий елемент є важливим для моніторингу адміністративної активності, оскільки використання `sudo` часто пов'язане зі зміною системних параметрів або виконанням привілейованих дій.

Правий блок дашборда деталізує автентифікаційну активність за користувачами та IP-адресами. Top Target Users показує облікові записи, які найчастіше фігурують у подіях автентифікації. Це дозволяє швидко виявити користувачів, щодо яких спостерігається підвищена кількість подій, наприклад `root`, `ubuntu` або інші системні чи локальні облікові записи. Top Source IPs відображає IP-адреси, з яких надходила найбільша кількість подій автентифікації.

У нижній частині розміщено таблицю Failed Login Events Table, яка надає деталізований перегляд окремих невдалих спроб автентифікації. У ній відображаються час події, IP-адреса джерела, користувач, опис правила та декодер, який обробив подію. Табличний формат дозволяє перейти від загальної статистики до конкретних повідомлень і визначити, з якого вузла або під яким обліковим записом було зафіксовано невдалу спробу входу.

Графік Authentication Events Over Time узагальнює події автентифікації за категоріями, зокрема успішні, невдалі та інші пов'язані з автентифікацією події. Завдяки цьому можна оцінити співвідношення між штатною активністю користувачів і потенційно проблемними подіями. Якщо кількість невдалих спроб різко зростає порівняно з успішними входами, це може бути підставою для подальшого аналізу в межах сценаріїв тестування.

Підсумовуючи, дашборд Authentication забезпечує окремий рівень контролю подій, пов'язаних із доступом користувачів до системи. Він дозволяє аналізувати джерела підключень, облікові записи, `sudo`-активність, SSH-події та невдалі спроби входу, що є важливим для виявлення потенційних спроб несанкціонованого доступу та контролю адміністративної активності.

Дашборд Rule & Severity Analysis призначений для аналізу правил Wazuh, рівнів критичності подій та структури спрацювань у підсистемі. Якщо попередні дашборди орієнтовані на загальний стан, мережеву активність і автентифікацію, то

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

цей екран деталізує саме аналітичну частину обробки подій: які правила спрацьовують найчастіше, які рівні критичності переважають і які групи правил формують основний обсяг повідомлень безпеки.



Рисунок 2.17 Rule & Severity Analysis

У верхній частині розміщено зведені показники, що характеризують стан правил та критичності подій за вибраний період. Highest Severity Detected показує найвищий рівень критичності, який був зафіксований у системі. Це дозволяє швидко визначити максимальний рівень потенційної загрози без перегляду всього журналу подій. Unique Rule IDs Triggered відображає кількість унікальних правил Wazuh, які спрацювали за обраний часовий проміжок, а Most Common Severity показує рівень критичності, що зустрічається найчастіше. Показник Total Rule Groups використовується для оцінювання кількості груп правил, задіяних у процесі аналізу подій.

Блок Alerts by Severity Over Time відображає зміну кількості подій різних рівнів критичності у часі. Такий графік дозволяє простежити не лише загальне зростання або зменшення кількості подій, а й те, які саме рівні критичності формують ці зміни. Наприклад, зростання кількості подій середнього або високого

рівня може свідчити про зміну характеру активності в мережі та потребує подальшого аналізу.

Елемент Severity Distribution показує загальний розподіл подій за рівнями критичності. Він доповнює часовий графік і дозволяє оцінити, які рівні подій переважають у системі в межах вибраного періоду. У поєднанні з показником найвищої критичності це дає змогу швидко оцінити загальний профіль ризику підсистеми.

Для аналізу правил використовується блок Top Triggered Rules, який відображає правила Wazuh, що спрацювали найчастіше. Така візуалізація дозволяє визначити типові або повторювані події в системі, наприклад, повідомлення про системні зміни, події автентифікації, встановлення пакетів або помилки служб. Це корисно для виявлення найбільш активних категорій подій і розуміння того, які саме правила формують основне навантаження в журналі безпеки.

Окремо реалізовано візуалізацію Rule IDs Frequency, яка показує частоту спрацювання конкретних ідентифікаторів правил. На відміну від описів правил, ідентифікатори дозволяють точніше пов'язати події з конкретними правилами Wazuh і використовувати їх для подальшої фільтрації або аналізу. Такий підхід є зручним у випадках, коли різні події мають подібні описи, але належать до різних правил.

Візуалізація Rule Groups by Severity поєднує аналіз груп правил із рівнями критичності. Вона дозволяє побачити, які групи правил формують події низького, середнього або високого рівня. Розмір маркера відображає кількість подій у відповідній групі, що дає змогу швидко визначити найбільш активні групи правил і їхній внесок у загальну картину критичності.

Таблиця Critical Alerts Table містить деталізований перелік подій із підвищеним рівнем критичності. Тут відображаються час події, агент, рівень критичності, опис правила та декодер. Такий формат дозволяє перейти від узагальнених показників до конкретних повідомлень безпеки, які потребують додаткового аналізу.

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				49
Змн.	Арк.	№ докум.	Підпис	Дата		

Дашборд Rule & Severity Analysis є основним інструментом для аналізу результатів роботи механізмів виявлення Wazuh. Він дозволяє оцінити, які правила спрацьовують найчастіше, які рівні критичності переважають, які групи правил є найбільш активними та які події потребують першочергової уваги.

У результаті реалізації системи візуалізації було створено набір інформаційних панелей, які забезпечують різні рівні аналізу подій безпеки: від загального огляду стану підсистеми до деталізованого аналізу автентифікації, мережевої активності, правил Wazuh та рівнів критичності. Це дозволяє розподілити інформацію за функціональними напрямками та уникнути перевантаження одного дашборда великою кількістю показників.

Використання єдиного індексу wazuh-alerts та структурованих JSON-подій забезпечує узгодженість даних між усіма інформаційними панелями. Завдяки цьому користувач може переходити від загальних числових показників до конкретних таблиць подій, аналізувати джерела активності, оцінювати рівні критичності та визначати правила, які спрацьовують найчастіше.

Висновки до розділу

У другому розділі було виконано проєктування та реалізацію підсистеми аналізу подій безпеки гетерогенної мережі. Було визначено структуру мережевого середовища, до складу якого входять сервер Wazuh, сервер Splunk Enterprise, Windows та Linux хости, а також шлюз на базі pfSense для організації взаємодії внутрішнього сегмента мережі із зовнішнім середовищем.

Було розгорнуто та налаштовано основні компоненти підсистеми: сервер Wazuh, агенти моніторингу, сервер Splunk Enterprise та Splunk Universal Forwarder. Wazuh використовується для збору й первинної обробки подій безпеки, а Splunk Enterprise – для їх індексації, пошуку, аналізу та візуалізації. Для передавання подій між Wazuh і Splunk було налаштовано моніторинг файлу alerts.json, у якому зберігаються сформовані Wazuh повідомлення безпеки, та передавання даних до індексу wazuh-alerts.

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

У межах реалізації механізму централізованого збору було описано проходження подій від кінцевих вузлів до Wazuh Manager, їх обробку за допомогою декодерів і правил Wazuh, формування структурованих JSON-повідомлень та подальшу передачу до Splunk. Окремо було розглянуто основні поля подій, які використовуються для фільтрації, групування, побудови пошукових запитів та подальшого аналізу.

Також було реалізовано систему візуалізації у Splunk Enterprise. Для цього створено набір інформаційних панелей, призначених для загального огляду стану підсистеми, моніторингу мережевої активності, аналізу подій автентифікації, а також оцінювання правил Wazuh і рівнів критичності. Такий підхід дозволяє організувати багаторівневий моніторинг подій безпеки та перейти від загальної оцінки стану системи до детального аналізу окремих категорій подій.

У результаті виконання другого розділу було реалізовано повноцінну основу підсистеми централізованого аналізу подій безпеки, яка забезпечує збір, обробку, передачу, індексацію та візуалізацію подій із вузлів гетерогенної мережі. Отримана система є підготовленою до подальшого практичного дослідження її роботи під час моделювання подій безпеки та аналізу результатів у третьому розділі.

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				51
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3 ТЕСТУВАННЯ ТА ОЦІНЮВАННЯ РОБОТИ ПІДСИСТЕМИ АНАЛІЗУ ПОДІЙ БЕЗПЕКИ

3.1 Моделювання інцидентів безпеки в гетерогенній мережі

Для дослідження роботи реалізованої підсистеми було змодельовано декілька інцидентів безпеки, що охоплюють різні типи активності в гетерогенній мережі. Моделювання виконувалося після завершення розгортання основних компонентів підсистеми, налаштування агентів Wazuh, передавання подій до Splunk Enterprise та створення інформаційних панелей моніторингу. Такий підхід дозволяє перевірити роботу підсистеми не лише на рівні окремого компонента, а як цілісного ланцюга збору, обробки, передавання, індексації та візуалізації подій безпеки.

Окремо для моделювання дій порушника було використано віртуальну машину Kali Linux. Цей дистрибутив орієнтований на тестування безпеки та містить інструменти для перевірки захищеності мережевих сервісів, зокрема засоби для сканування, аналізу доступності вузлів і підбору облікових даних. У роботі ця віртуальна машина застосовувалася не як штатний вузол інфраструктури, а як джерело контрольованих дій, характерних для внутрішнього порушника. Це дозволяє змодельовати ситуацію, коли зловмисник уже отримав початкову присутність у мережі та виконує подальші дії щодо інших вузлів інфраструктури. У контексті тестування це дає змогу перевірити здатність підсистеми фіксувати не лише звичайну активність кінцевих хостів, а й підозрілі дії, що виникають усередині мережевого сегмента.

Основним сценарієм було обрано спробу підбору пароля до SSH-сервісу Linux-хоста. SSH використовується для віддаленого адміністрування Linux-систем і часто є ціллю атак підбору облікових даних. Для моделювання такої активності застосовувався інструмент Hydra на Kali Linux. Його використання дозволяє сформувати послідовність невдалих спроб автентифікації до цільового сервісу з одного джерела. На відміну від одиничного неправильного введення пароля, така

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		52

активність має характер повторюваної атаки та формує серію подій, придатних для аналізу засобами Wazuh і Splunk.

Для уникнення фактичної компрометації облікового запису тестовий словник паролів було сформовано без правильного пароля користувача. Це дозволило змодельовати процес підбору облікових даних без успішного входу до системи. У результаті такого сценарію очікується формування подій, пов'язаних із невдалою автентифікацією, зверненням до SSH-сервісу, фіксацією джерела підключення та повторюваністю спроб доступу.

```
(kali@kali)-[~]
$ hydra -l ubuntu -P passwords.txt ssh://194.42.4.102 -t 2 -V
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is n
on-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-05-21 09:
45:22
[DATA] max 2 tasks per 1 server, overall 2 tasks, 7 login tries (l:1/p:7), ~4
tries per task
[DATA] attacking ssh://194.42.4.102:22/
[ATTEMPT] target 194.42.4.102 - login "ubuntu" - pass "123456" - 1 of 7 [chil
d 0] (0/0)
[ATTEMPT] target 194.42.4.102 - login "ubuntu" - pass "password" - 2 of 7 [ch
ild 1] (0/0)
[ATTEMPT] target 194.42.4.102 - login "ubuntu" - pass "qwerty" - 3 of 7 [chil
d 0] (0/0)
[ATTEMPT] target 194.42.4.102 - login "ubuntu" - pass "admin" - 4 of 7 [child
1] (0/0)
[ATTEMPT] target 194.42.4.102 - login "ubuntu" - pass "letmein" - 5 of 7 [chi
ld 0] (0/0)
[ATTEMPT] target 194.42.4.102 - login "ubuntu" - pass "test123" - 6 of 7 [chi
ld 1] (0/0)
[ATTEMPT] target 194.42.4.102 - login "ubuntu" - pass "111111" - 7 of 7 [chil
d 0] (0/0)
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-05-21 09:
45:34
```

Рисунок 3.1 – Моделювання спроб підбору пароля до SSH-сервісу за допомогою Hydra

Другий сценарій спрямований на моделювання адміністративної активності на Linux-хості. Цей сценарій не є прямою атакою на мережевий сервіс, однак він важливий для оцінювання здатності підсистеми фіксувати дії користувачів усередині операційної системи. Для цього виконувалися команди з використанням sudo, а також дії, пов'язані зі створенням і видаленням тестового користувача. Така

активність може бути частиною штатного адміністрування, але в контексті інциденту безпеки також може свідчити про дії після отримання доступу до вузла.

На першому етапі було виконано декілька команд із підвищеними привілеями: визначення поточного користувача, перегляд вмісту каталогу /root та перевірка стану SSH-служби. Такі дії дозволяють сформувати події, пов'язані з використанням механізму sudo, відкриттям привілейованої сесії та зверненням до системних служб Linux-хоста.

```
ubuntu@ubuntu2204:~$ sudo whoami
root
ubuntu@ubuntu2204:~$ sudo ls /root
snap
ubuntu@ubuntu2204:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: enabled)
   Active: active (running) since Thu 2026-05-21 16:29:45 EEST; 17min ago
 TriggeredBy: ● ssh.socket
    Docs: man:sshd(8)
          man:sshd_config(5)
   Process: 8268 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
  Main PID: 8280 (sshd)
    Tasks: 1 (limit: 1033)
  Memory: 204.0K (peak: 13.9M swap: 1.0M swap peak: 1.1M)
     CPU: 693ms
    CGroup: /system.slice/ssh.service
            └─8280 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"
```

Рисунок 3.2 – Формування адміністративних подій на Linux-хості за допомогою sudo

Адміністративна активність на Linux-хості дозволяє перевірити фіксацію подій, які не мають зовнішнього мережевого джерела, але є важливими для аналізу стану системи. На відміну від сценарію підбору пароля, такі події виникають без взаємодії з віддаленим вузлом і характеризують локальні дії користувача в операційній системі. Їх фіксація є важливою, оскільки після отримання доступу до вузла порушник може виконувати команди з підвищеними привілеями, переглядати системні каталоги або перевіряти стан служб.

Окремо було змодельовано зміну стану облікових записів користувачів. Для цього на Linux-хості було створено тестового користувача testuser, після чого виконувалися дії, пов'язані з його налаштуванням і подальшим видаленням. Такі

операції дозволяють сформувати події, пов'язані з керуванням користувачами, що є важливим для контролю змін у системі облікових записів.

```
ubuntu@ubuntu2204:~$ sudo adduser testuser
info: Adding user `testuser' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `testuser' (1002) ...
info: Adding new user `testuser' (1002) with group `testuser (1002)' ...
info: Creating home directory `/home/testuser' ...
info: Copying files from `/etc/skel' ...
New password:
```

Рисунок 3.3 – Створення тестового користувача на Linux-хості

Наявність таких повідомлень у системі моніторингу дає змогу використовувати підсистему не лише для виявлення атак на мережеві сервіси, а й для контролю локальної активності користувачів. Це особливо важливо для сценаріїв, у яких підозріла активність проявляється не через мережеві підключення, а через зміну стану системи, виконання адміністративних команд або створення нових облікових записів.

Третій сценарій пов'язаний із Windows-хостом. Windows-події мають іншу структуру журналів, інші джерела подій та інший формат представлення інформації. Тому моделювання активності Windows-хоста дозволяє перевірити надходження подій цієї операційної системи до Wazuh і можливість їх подальшого централізованого аналізу у Splunk.

Для Windows-хоста було сформовано дві групи подій: події автентифікації користувача та системні події операційної системи. Події автентифікації створювалися шляхом виконання успішних і невдалих спроб входу користувача. Вони потрібні для перевірки того, як підсистема фіксує спроби доступу до Windows-хоста та як такі повідомлення надалі відображаються разом із Linux-подіями автентифікації.

Окремо було змодельовано системну активність Windows-хоста, пов'язану зі зміною стану служби. Для цього в PowerShell було виконано зупинку та повторний запуск служби Spooler, яка відповідає за роботу черги друку в Windows. Така дія дозволяє сформувати системні події Windows і перевірити, чи обробляються вони агентом Wazuh.

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		55

```
PS C:\Windows\system32> Get-Service Spooler

Status      Name      DisplayName
-----
Running     Spooler    Print Spooler

PS C:\Windows\system32> stop-Service Spooler
PS C:\Windows\system32> start-Service Spooler
PS C:\Windows\system32>
```

Рисунок 3.4 – Формування системних подій Windows шляхом зміни стану служби

Зміна стану системної служби використовується як контрольований спосіб створення подій Windows Event Log. Такі події важливі для перевірки роботи підсистеми з журналами Windows, оскільки в реальних умовах зміна стану служб може бути як штатною адміністративною дією, так і ознакою небажаної активності в системі.

Для кожного сценарію фіксувалися дії, які призводили до появи подій. На стороні Wazuh ці події збиралися агентами, проходили первинну обробку та перетворювалися на структуровані повідомлення безпеки. Подальший аналіз виконувався у Splunk, куди події передавалися через Splunk Universal Forwarder. Оцінювання результатів здійснювалося за наявністю подій в індексі wazuh-alerts, коректністю основних полів, рівнем критичності та відображенням у дашбордах.

Обрані сценарії охоплюють декілька важливих напрямів моніторингу: спробу підбору пароля до мережевого сервісу, локальну адміністративну активність у Linux-системі та події Windows-хоста. Це забезпечує різноманітність тестових даних і дозволяє оцінити роботу підсистеми в умовах гетерогенної інфраструктури, де події безпеки можуть формуватися з різних джерел і мати різну структуру.

3.2 Аналіз результатів виявлення подій

Після моделювання інцидентів сформовані події були передані до Splunk Enterprise через індекс wazuh-alerts. Аналіз результатів виконувався за допомогою SPL-запитів, які дозволяють відфільтрувати події за джерелом, агентом, декодером, описом правила та додатковими полями, сформованими Wazuh. Основна увага приділялася тому, чи зберігають події після індексації необхідні атрибути для

подальшого аналізу: час виникнення, назву агента, рівень критичності, ідентифікатор правила, опис події, IP-адресу джерела, користувача та назву декодера.

Першим було проаналізовано результати моделювання спроби підбору пароля до SSH-сервісу Linux-хоста. Оскільки джерелом контрольованої активності виступала віртуальна машина Kali Linux з IP-адресою 194.42.4.150, для пошуку відповідних подій у Splunk було використано фільтрацію за полем data.srccip. Це дозволяє відокремити події, пов'язані саме з діями цього вузла, від інших журналів, що надходять до індексу wazuh-alerts.

Для перегляду подій, сформованих у результаті спроб підбору пароля, було використано запит, який виводить основні атрибути повідомлень безпеки: час події, назву агента, рівень критичності, ідентифікатор правила, опис спрацьованого правила, IP-адресу джерела, цільового користувача та декодер.

New Search SPL Convert to SPL2 Save As Create Table View Close

index=wazuh-alerts sourcetype=wazuh-alerts
 | spath
 | search data.srccip="194.42.4.150"
 | table _time agent.name rule.level rule.id rule.description data.srccip data.dstuser decoder.name
 | sort - _time

Time range: Last 24 hours

✓ 20 events (5/20/26 4:00:00.000 PM to 5/21/26 4:53:51.000 PM) No Event Sampling Job

Events Patterns **Statistics (20)** Visualization

Show: 50 Per Page Format Preview: On

_time	agent.name	rule.level	rule.id	rule.description	data.srccip	data.dstuser	decoder.name
2026-05-21 16:45:34.847	ubuntu2204	10	2502	syslog: User missed the password more than one time	194.42.4.150	ubuntu	sshd
2026-05-21 16:45:34.834	ubuntu2204	5	5760	sshd: authentication failed.	194.42.4.150	ubuntu	sshd
2026-05-21 16:45:32.836	ubuntu2204	10	2502	syslog: User missed the password more than one time	194.42.4.150	ubuntu	sshd
2026-05-21 16:45:30.835	ubuntu2204	5	5760	sshd: authentication failed.	194.42.4.150	ubuntu	sshd
2026-05-21 16:45:30.831	ubuntu2204	5	5760	sshd: authentication failed.	194.42.4.150	ubuntu	sshd

Рисунок 3.5 – Події SSH-автентифікації, сформовані внаслідок активності Kali Linux

На рисунку видно, що всі відібрані події мають значення `data.srcip = 194.42.4.150`, тобто пов'язані з вузлом Kali Linux. Як агент-джерело подій визначено `ubuntu2204`, що відповідає Linux-хосту, на якому працює SSH-сервіс. У полі `data.dstuser` відображається користувач `ubuntu`, до якого виконувалися спроби автентифікації. Це підтверджує, що події були сформовані саме на цільовому Linux-хості внаслідок звернень до SSH-служби.

Важливо, що для цього сценарію події відфільтровано саме за IP-адресою джерела, а не лише за назвою агента або описом правила, адже це дозволяє відокремити активність Kali Linux від інших подій, які паралельно могли формуватися в системі. Оскільки в індекс `wazuh-alerts` надходять повідомлення з різних вузлів, фільтрація за `data.srcip` є зручним способом виділити події, пов'язані з конкретним джерелом підозрілої активності. Це особливо важливо для сценаріїв підбору пароля, де ключовими ознаками є повторювані спроби доступу з однієї адреси до одного облікового запису.

Опис правил Wazuh вказує на невдалі спроби автентифікації та повторювані помилки введення пароля. Зокрема, у результатах присутні повідомлення типу «`sshd: authentication failed`» та «`syslog: User missed the password more than one time`». Такі події відображають характерну поведінку під час підбору пароля, коли з одного джерела виконується серія спроб входу до одного облікового запису. Наявність декодера `sshd` свідчить про те, що Wazuh коректно класифікував ці повідомлення як події SSH-служби.

Окрему увагу слід звернути на рівні критичності подій. У результатах присутні події з рівнями 5 та 10. Події нижчого рівня відповідають окремим невдалим спробам автентифікації, тоді як вищий рівень пов'язаний із повторюваністю помилок введення пароля. Це дозволяє не лише зафіксувати сам факт невдалої автентифікації, а й виділити більш підозрілу активність, яка має ознаки багаторазового підбору облікових даних.

Для узагальнення отриманих результатів було використано агрегований запит, який групує події за описом правила, рівнем критичності, ідентифікатором правила та декодером. Групування подій за цими атрибутами дозволяє визначити,

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		58

які саме правила Wazuh спрацьовували найчастіше під час моделювання атаки, а також оцінити співвідношення між окремими типами подій.

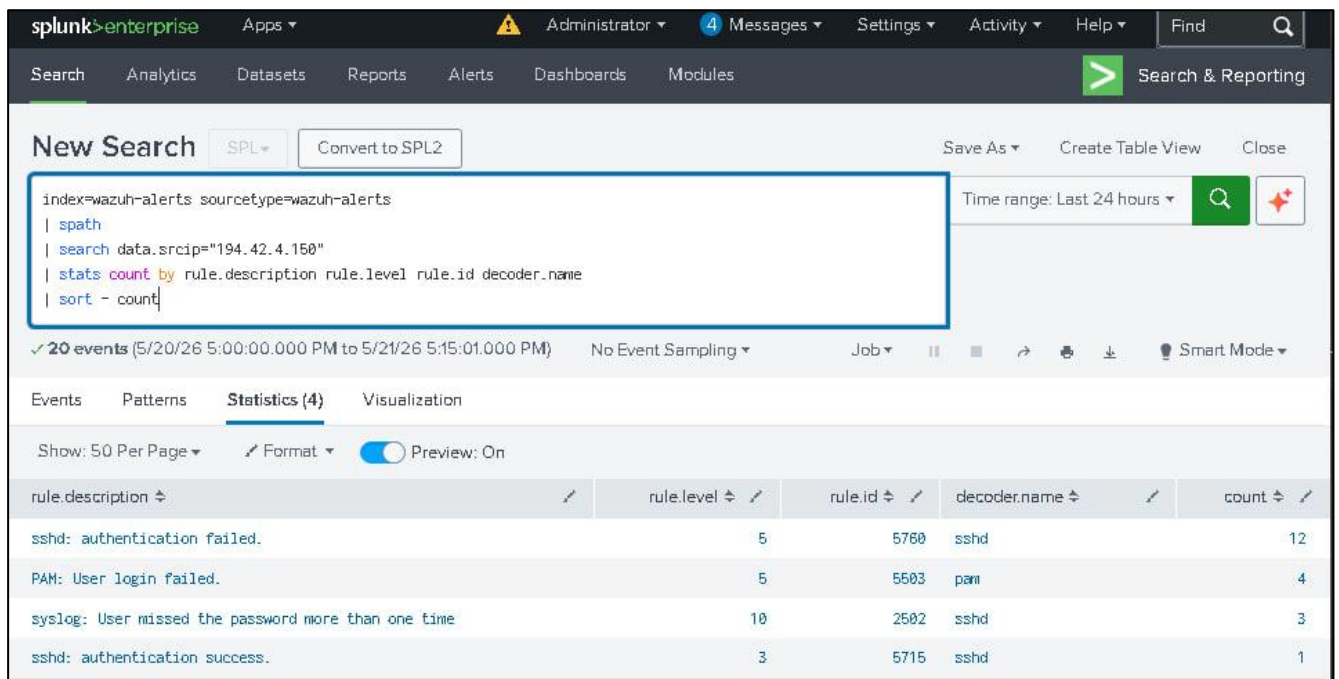


Рисунок 3.6 – Агрегація подій SSH brute-force за правилами Wazuh

У результатах агрегації видно, що найбільшу кількість подій сформовано для правила «sshd: authentication failed», яке відповідає невдалим спробам автентифікації в SSH. Також присутні події «PAM: User login failed», що пов'язані з механізмом автентифікації PAM у Linux, та події про багаторазово пропущений пароль. Це показує, що одна серія спроб входу може бути представлена кількома взаємопов'язаними повідомленнями, оскільки SSH-служба та PAM формують різні журнальні записи для одного процесу автентифікації.

Отримані результати демонструють, що Wazuh не лише фіксує окремі невдалі спроби входу, а й формує події з різними правилами та рівнями критичності залежно від характеру повідомлення. Після передавання до Splunk ці події зберігають структуровані поля, необхідні для подальшого аналізу: IP-адресу джерела, цільового користувача, агента, декодер, опис правила та рівень критичності. Це дозволяє використовувати їх для пошуку, агрегації, побудови таблиць і відображення у дашбордах моніторингу.

Отримані результати підтверджують, що сценарій SSH brute-force був коректно зафіксований у підсистемі. Події, сформовані на Linux-хості, пройшли

первинну обробку у Wazuh, були передані до Splunk і стали доступними для подальшого аналізу через індекс wazuh-alerts. Наявність поля data.srcip дозволила однозначно визначити джерело активності, а поля rule.description, rule.level і decoder.name – оцінити характер подій та їхню критичність.

Наступним етапом було проаналізовано події, сформовані внаслідок адміністративної активності на Linux-хості. На відміну від попереднього сценарію, ці події не пов'язані з віддаленою спробою доступу з окремого вузла, а виникають безпосередньо в операційній системі під час виконання користувачем привілейованих дій. Для їх пошуку було використано фільтрацію за агентом ubuntu2204 та ознаками, характерними для sudo-подій.

Запит було сформовано так, щоб відібрати події, пов'язані з використанням механізму sudo, виконанням команд від імені привілейованого користувача та переходом до контексту root.

The screenshot shows the Splunk Enterprise web interface. At the top, there's a navigation bar with 'splunk>enterprise' and various menu items like 'Apps', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and a 'Find' search bar. Below this is a secondary navigation bar with 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', 'Dashboards', and 'Modules'. The main content area is titled 'New Search' and contains a search bar with the following query: `index=wazuh-alerts sourcetype=wazuh-alerts | spath | search agent.name="ubuntu2204" (decoder.name=sudo OR rule.description="*sudo*" OR rule.description="*ROOT*") | table _time agent.name rule.level rule.id rule.description data.dstuser data.srcuser decoder.name | sort - _time`. To the right of the search bar, there's a 'Time range: Yesterday' dropdown and a search button. Below the search bar, it shows '6 events (5/21/26 12:00:00.000 AM to 5/22/26 12:00:00.000 AM)'. The results are displayed in a table with columns: _time, agent.name, rule.level, rule.id, rule.description, data.dstuser, data.srcuser, and decoder.name. The table shows six rows of events, all with the same details: agent.name 'ubuntu2204', rule.level '3', rule.id '5402', rule.description 'Successful sudo to ROOT executed.', data.dstuser 'root', data.srcuser 'ubuntu', and decoder.name 'sudo'.

_time	agent.name	rule.level	rule.id	rule.description	data.dstuser	data.srcuser	decoder.name
2026-05-21 16:47:58.944	ubuntu2204	3	5402	Successful sudo to ROOT executed.	root	ubuntu	sudo
2026-05-21 16:47:48.938	ubuntu2204	3	5402	Successful sudo to ROOT executed.	root	ubuntu	sudo
2026-05-21 16:47:18.921	ubuntu2204	3	5402	Successful sudo to ROOT executed.	root	ubuntu	sudo
2026-05-21 16:47:02.912	ubuntu2204	3	5402	Successful sudo to ROOT executed.	root	ubuntu	sudo
2026-05-21 16:46:50.902	ubuntu2204	3	5402	Successful sudo to ROOT executed.	root	ubuntu	sudo
2026-05-21 16:46:42.907	ubuntu2204	3	5402	Successful sudo to ROOT executed.	root	ubuntu	sudo

Рисунок 3.7 – Події виконання команд із підвищеними привілеями на Linux-хості

На рисунку видно, що події сформовані агентом ubuntu2204, тобто Linux-хостом, на якому виконувалися адміністративні команди. У полі rule.description відображається повідомлення «Successful sudo to ROOT executed», що вказує на успішне виконання команди з підвищеними привілеями. Поле data.srcuser містить користувача ubuntu, який ініціював дію, а поле data.dstuser – користувача root, від імені якого було виконано команду. Наявність декодера sudo свідчить про те, що Wazuh коректно класифікував ці журнальні записи як події використання механізму sudo.

Такі повідомлення мають важливе значення для моніторингу безпеки, оскільки виконання команд із підвищеними привілеями може бути як частиною штатного адміністрування, так і ознакою небажаної активності після отримання доступу до системи. Сам факт успішного виконання sudo не є інцидентом, однак у поєднанні з іншими подіями, наприклад невдалими спробами входу або зміною облікових записів, така активність може потребувати додаткової уваги.

Окремо було проаналізовано події, пов'язані з механізмом PAM. Для цього було використано запит, який відбирає події агента ubuntu2204, оброблені декодером pam.

New Search							
index=wazuh-alerts sourcetype=wazuh-alerts spath search agent.name="ubuntu2204" decoder.name=pam table _time agent.name rule.level rule.id rule.description data.dstuser data.srcuser decoder.name sort - _time							
20 events (5/21/26 12:00:00.000 AM to 5/22/26 12:00:00.000 AM)							
Statistics (20)							
_time	agent.name	rule.level	rule.id	rule.description	data.dstuser	data.srcuser	decoder.name
2026-05-21 16:47:56.966	ubuntu2204	3	5502	PAM: Login session closed.	root		pam
2026-05-21 16:47:56.944	ubuntu2204	3	5501	PAM: Login session opened.	root	ubuntu	pam

Рисунок 3.8 – Події PAM-сесій на Linux-хості

У результатах відображаються події відкриття та закриття користувацької сесії. Вони доповнюють sudo-події та дозволяють відстежувати не лише факт виконання привілейованої команди, а й супровідні автентифікаційні процеси, які виникають під час роботи користувача в системі. Поля rule.description, data.srcuser, data.dstuser та decoder.name дають змогу визначити характер дії, користувача, пов'язаного з подією, та механізм, який сформував відповідний журнальний запис.

Для аналізу змін у системі облікових записів було використано окремий запит до поля full_log. Це поле містить початковий журнальний запис, тому дозволяє знаходити події, пов'язані з командами створення або видалення користувачів.

The screenshot displays the Splunk Enterprise search interface. The search bar contains the following query:

```
index=wazuh-alerts sourcetype=wazuh-alerts
| spath
| search agent.name='ubuntu2204' (
  full_log='*adduser*' OR full_log='*useradd*' OR full_log='*userdel*'
)
| table _time agent.name rule.level rule.id rule.description full_log decoder.name
| sort - _time
```

The results table shows the following data:

_time	agent.name	rule.level	rule.id	rule.description	full_log	decoder.name
2026-05-21 16:47:56.944	ubuntu2204	3	5402	Successful sudo to ROOT executed.	May 21 13:47:55 ubuntu2204 sudo[9332]: ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/sbin/userdel testuser	sudo
2026-05-21 16:47:56.944	ubuntu2204	3	5903	Group (or user) deleted from the system.	May 21 13:47:55 ubuntu2204 userdel[9334]: delete user 'testuser'	open-userdel
2026-05-21 16:47:48.938	ubuntu2204	3	5402	Successful sudo to ROOT executed.	May 21 13:47:48 ubuntu2204 sudo[9329]: ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/sbin/userdel testuser	sudo
2026-05-21 16:47:28.941	ubuntu2204	8	5902	New user added to the system.	May 21 13:47:19 ubuntu2204 useradd[9287]: new user: name=testuser, UID=1002, GID=1002, home=/home/testuser, shell=/bin/bash, from=/dev/pts/1	useradd

Рисунок 3.9 – Події створення та видалення користувача на Linux-хості

На рисунку видно, що підсистема зафіксувала створення та видалення тестового користувача testuser. Подія «New user added to the system» відображає створення нового облікового запису, а повідомлення «Group (or user) deleted from the system» відповідає його подальшому видаленню. У полі full_log містяться деталі

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				62
Змн.	Арк.	№ докум.	Підпис	Дата		

виконаної дії, зокрема ім'я користувача, ідентифікатори UID та GID, домашній каталог і команда, що була виконана.

Цей результат доповнює події sudo та pam, оскільки дозволяє простежити не тільки факт виконання команд із підвищеними привілеями, а й наслідки таких дій для конфігурації системи. У контексті централізованого аналізу події керування користувачами є важливими, оскільки створення нового облікового запису або його видалення може бути як штатною адміністративною дією, так і ознакою небажаної активності після отримання доступу до вузла.

На відміну від подій SSH brute-force, адміністративні події Linux-хоста не обов'язково містять IP-адресу джерела. Це пояснюється тим, що вони формуються локально в операційній системі та описують дії користувача після входу в систему. Тому для їх аналізу важливішими є не мережеві атрибути, а поля, пов'язані з користувачем, цільовим привілейованим обліковим записом, описом правила та декодером.

Отримані результати демонструють, що підсистема фіксує не лише події, пов'язані з мережевими спробами доступу, а й локальну адміністративну активність Linux-хоста. Це важливо для аналізу сценаріїв, у яких підозріла поведінка проявляється вже після входу користувача до системи. Події sudo та pam дозволяють відстежувати виконання привілейованих команд, відкриття сесій і взаємодію користувача з механізмами автентифікації Linux.

Далі було проаналізовано події Windows-хоста. На відміну від Linux-подій, які в попередніх сценаріях оброблялися декодерами sshd, sudo та pam, події Windows надходять із журналів Windows Event Log і обробляються декодером windows_eventchannel. Тому для їх аналізу було використано фільтрацію за відповідним декодером та ознаками, пов'язаними з автентифікацією користувача.

Для перегляду подій входу було сформовано запит, який відбирає повідомлення Windows хоста, пов'язані з успішними та невдалими спробами автентифікації. У запиті додатково створено поле auth_status, яке дозволяє подати результат входу у вигляді Successful або Failed, що спрощує подальший аналіз,

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		63

оскільки статус автентифікації відображається окремою колонкою, а не лише в описі правила.

```

index=wazuh-alerts sourcetype=wazuh-alerts
| spath
| search decoder.name="windows_eventchannel" (data.win.system.eventID=4624 OR data.win.system.eventID=4625)
| eval auth_status=case(
  'data.win.system.eventID'=4624, "Successful",
  'data.win.system.eventID'=4625, "Failed",
  true(), "Other"
)
| table _time agent.name auth_status rule.level rule.id rule.description data.win.system.eventID data.win.eventdata.targetUserName
| sort - _time
  
```

_time	agent.name	auth_status	rule.level	rule.id	rule.description	data.win.system.eventID	data.win.eventdata.targetUserName
2026-05-22 14:03:19.645	DESKTOP-V3EKL0Q	Successful	3	60118	Windows Workstation Logon Success	4624	Student
2026-05-22 14:03:19.642	DESKTOP-V3EKL0Q	Successful	3	60118	Windows Workstation Logon Success	4624	Student
2026-05-22 14:03:16.789	DESKTOP-V3EKL0Q	Failed	5	60122	Logon Failure - Unknown user or bad password	4625	Student
2026-05-22	DESKTOP-V3EKL0Q	Failed	5	60122	Logon Failure	4625	Student

Рисунок 3.10 – Події автентифікації Windows-хоста у Splunk

На рисунку видно, що події сформовані агентом DESKTOP-V3EKL0Q, який відповідає Windows-хосту. У результатах присутні як успішні, так і невдалі спроби входу користувача Student. Поле auth_status дозволяє швидко відокремити успішні входи від помилок автентифікації, а поле rule.description містить текстовий опис події. Для невдалих спроб у результатах відображається повідомлення про помилку входу, пов'язану з невідомим користувачем або неправильним паролем.

Наявність поля data.win.system.eventID дозволяє співвіднести події з відповідними ідентифікаторами Windows Event Log. У цьому випадку події успішного та невдалого входу мають різні ідентифікатори, що дає змогу відокремлювати їх у запитах і дашбордах. Це важливо для подальшого аналізу, оскільки журнали Windows містять велику кількість подій, і без додаткової фільтрації автентифікаційні повідомлення можуть змішуватися з іншими системними записами.

Окремо слід зазначити, що Windows-події мають іншу структуру полів порівняно з Linux-подіями. Якщо для SSH brute-force основними атрибутами були data.srcip, data.dstuser та decoder.name, то для Windows-подій важливими є поля з групи data.win, зокрема ідентифікатор події, канал журналу та ім'я користувача. Це підтверджує необхідність використання окремих умов фільтрації для різних операційних систем у межах єдиної системи аналізу.

Крім подій автентифікації, було проаналізовано системні події Windows-хоста, сформовані під час зміни стану служби. Для цього використовувався запит, що відбирає повідомлення, пов'язані із системним каналом Windows або службовими подіями. Такий підхід дозволяє перевірити, чи фіксує підсистема не лише входи користувачів, а й зміни в роботі системних компонентів операційної системи.

index=wazuh-alerts sourcetype=wazuh-alerts							
spath							
search decoder.name="windows_eventchannel" (rule.description="*service*" OR rule.description="*Service*" OR data.win.system.channel="System")							
table _time agent.name rule.level rule.id rule.description data.win.system.eventID data.win.system.channel							
sort - _time							
✓ 24 events (5/21/26 2:00:00.000 PM to 5/22/26 2:14:53.000 PM) No Event Sampling Job							
Events Patterns Statistics (24) Visualization							
Show: 50 Per Page Format Preview: On							
_time	agent.name	rule.level	rule.id	rule.description	data.win.system.eventID	data.win.system.channel	
2026-05-22 14:11:04.454	DESKTOP-V3EKL0Q	3	60642	Software protection service scheduled successfully.	16384	Application	
2026-05-22 14:08:36.119	DESKTOP-V3EKL0Q	3	60642	Software protection service scheduled successfully.	16384	Application	
2026-05-22 14:07:30.288	DESKTOP-V3EKL0Q	3	61104	Service startup type was changed	7040	System	
2026-05-22 14:05:47.665	DESKTOP-V3EKL0Q	5	61102	Windows System error event	10010	System	
2026-05-22 14:05:23.405	DESKTOP-V3EKL0Q	3	60642	Software protection service scheduled successfully.	16384	Application	
2026-05-22 14:04:55.733	DESKTOP-V3EKL0Q	3	61104	Service startup type was changed	7040	System	

Рисунок 3.11 – Системні події Windows-хоста, пов'язані зі службами

У результатах відображаються події Windows-хоста, оброблені декодером windows_eventchannel. Зокрема, серед них присутні повідомлення про зміну типу запуску служби, системні події Windows та службові повідомлення Software

Protection Service. Такі записи мають значення для моніторингу стану системи, оскільки зміна параметрів служб може бути як штатною адміністративною дією, так і частиною небажаної активності.

У таблиці також відображається рівень критичності та ідентифікатор правила Wazuh. Це дозволяє оцінити не лише сам факт появи події, а й те, як вона була класифікована системою. Події системної активності Windows переважно мають нижчий або середній рівень критичності, однак їх наявність у централізованому журналі є важливою для формування повної картини стану вузла.

Отримані результати демонструють, що підсистема здатна обробляти події Windows хоста разом із подіями Linux середовища. Події автентифікації дозволяють аналізувати спроби доступу користувачів, а системні події – контролювати зміни в роботі служб і компонентів операційної системи. Завдяки цьому реалізована підсистема може використовуватися для централізованого моніторингу гетерогенної мережі, у якій одночасно функціонують вузли з різними операційними системами.

3.3 Оцінювання роботи інформаційних панелей після моделювання інцидентів

Після моделювання інцидентів безпеки було оцінено роботу створених інформаційних панелей Splunk. На цьому етапі основна увага приділялася не окремим подіям, а тому, як результати тестування відображаються у зведеному вигляді. Це дозволяє перевірити, чи можуть дашборди використовуватися для швидкого виявлення змін у стані підсистеми, оцінювання активності вузлів, аналізу подій автентифікації та контролю рівнів критичності.

Для оцінювання використовувався часовий діапазон Last 24 hours, оскільки основні події тестування були сформовані протягом одного періоду. У цей проміжок потрапили події SSH brute-force з Kali Linux, адміністративна активність Linux-хоста та події Windows-хоста, що дозволяє розглядати всі змодельовані сценарії одночасно та порівнювати їхній вплив на різні елементи візуалізації.

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		66

На відміну від окремих SPL-запитів, інформаційні панелі дають змогу оцінити результати моделювання інцидентів у ширшому контексті. Окремий запит показує конкретну групу подій, тоді як дашборд відображає їхній вплив на загальні показники системи: кількість повідомлень, активність агентів, джерела підключень, рівні критичності та спрацювання правил Wazuh. Завдяки цьому можна швидко перейти від загального огляду стану підсистеми до детальнішого аналізу окремої категорії подій. Саме тому оцінювання дашбордів є важливим етапом перевірки практичної придатності реалізованої системи моніторингу.

Першою було розглянуто інформаційну панель Security Overview, яка виконує функцію загального огляду стану підсистеми після моделювання інцидентів.

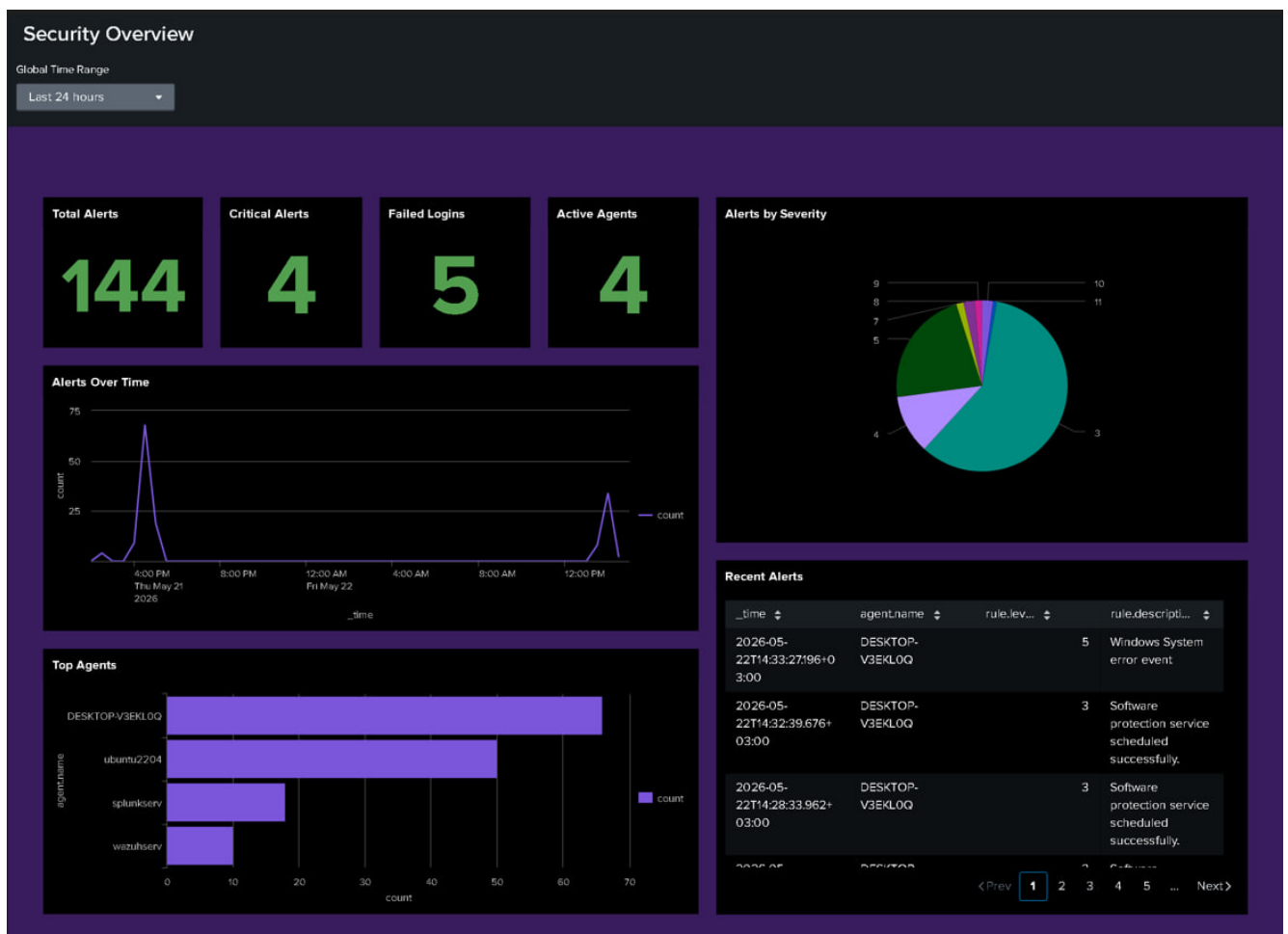


Рисунок 3.12 – Інформаційна панель Security Overview після моделювання інцидентів

На дашборді відображається загальна кількість подій за вибраний період, кількість критичних повідомлень, кількість невдалих входів та кількість активних

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				67
Змн.	Арк.	№ докум.	Підпис	Дата		

агентів. Показник Total Alerts демонструє загальний обсяг подій, отриманих від різних вузлів мережі. Значення Active Agents підтверджує, що події надходили від декількох джерел, зокрема Windows хоста, Linux хоста та серверних компонентів.

Показник Failed Logins відображає кількість згрупованих невдалих подій автентифікації. У цьому випадку він пов'язаний зі спробами підбору пароля до SSH-сервісу та невдалими входами Windows-користувача. Наявність цього показника на загальному дашборді дозволяє швидко помітити автентифікаційні проблеми без переходу до детальних пошукових запитів.

Графік Alerts Over Time показує нерівномірний розподіл подій у часі. На ньому видно сплески активності, які відповідають періодам генерації тестових сценаріїв. Це є важливим для моніторингу, оскільки різке збільшення кількості подій може вказувати на аномальну активність, наприклад серію невдалих спроб входу або виконання адміністративних дій.

Діаграма Alerts by Severity відображає розподіл подій за рівнями критичності Wazuh. Переважання подій нижчих і середніх рівнів свідчить про те, що більшість повідомлень стосувалася інформаційної або штатної системної активності. Водночас наявність подій вищих рівнів підтверджує, що змодельовані інциденти, зокрема повторювані спроби автентифікації, були класифіковані Wazuh як більш значущі для аналізу.

Елемент Top Agents дозволяє визначити, які вузли сформували найбільшу кількість подій. У результатах видно активність Windows хоста та Linux хоста, що відповідає проведенню сценаріям тестування. Таблиця Recent Alerts доповнює загальні показники та дає змогу переглянути останні повідомлення безпеки без виконання окремого SPL-запиту.

Такий розподіл також дає змогу оцінити, які вузли найбільше вплинули на загальну кількість подій. У цьому випадку активність Windows хоста пов'язана з подіями автентифікації та системними журналами, а активність Linux хоста – зі спробами SSH-автентифікації та адміністративними діями. Завдяки цьому загальний дашборд не лише показує кількість подій, а й допомагає визначити основні джерела активності в мережі.

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				68
Змн.	Арк.	№ докум.	Підпис	Дата		

Наступною було розглянуто інформаційну панель Authentication, орієнтовану на аналіз подій входу, SSH-активності, невдалих спроб автентифікації та дій користувачів.



Рисунок 3.13 – Інформаційна панель Authentication після моделювання інцидентів

Цей дашборд найбільш чітко відображає результати сценарію SSH brute-force. Показник SSH Events Count демонструє кількість подій, пов'язаних із SSH-службою, а Top Source IPs виділяє IP-адресу 194.42.4.150, з якої виконувалися спроби підбору пароля. Завдяки цьому можна швидко визначити джерело підозрілої активності без ручного перегляду всіх журналів.

Графік Failed Authentication Attempts відображає сплеск невдалих спроб автентифікації у момент виконання тестового сценарію. Така візуалізація є зручною для виявлення повторюваних помилок входу в короткий проміжок часу. У поєднанні з таблицею Failed Login Events Table вона дозволяє перейти від загальної динаміки до конкретних подій, у яких зазначено джерело, користувача, опис правила та декодер.

Показник Authentication Failure Rate у реалізованому дашборді використовується як кількісний індикатор згрупованих невдалих подій автентифікації. Він використовується для швидкої оцінки кількості невдалих автентифікаційних епізодів за вибраний період. Такий підхід дозволяє уникнути завищення показника через те, що одна фактична спроба входу може створювати декілька взаємопов’язаних Wazuh-повідомлень.

Елемент Top Target Users показує користувачів, які найчастіше фігурували у подіях автентифікації. У результатах присутній користувач ubuntu, що відповідає сценарію підбору пароля до SSH-сервісу Linux-хоста. Також у дашборді відображаються інші користувачі, пов’язані з адміністративною активністю та Windows-подіями, що підтверджує об’єднання подій різних операційних систем у спільному середовищі моніторингу.

Дашборд Network Activity використовується для оцінювання мережевої активності та подій, у яких присутні IP-адреси або мережеві декодери.

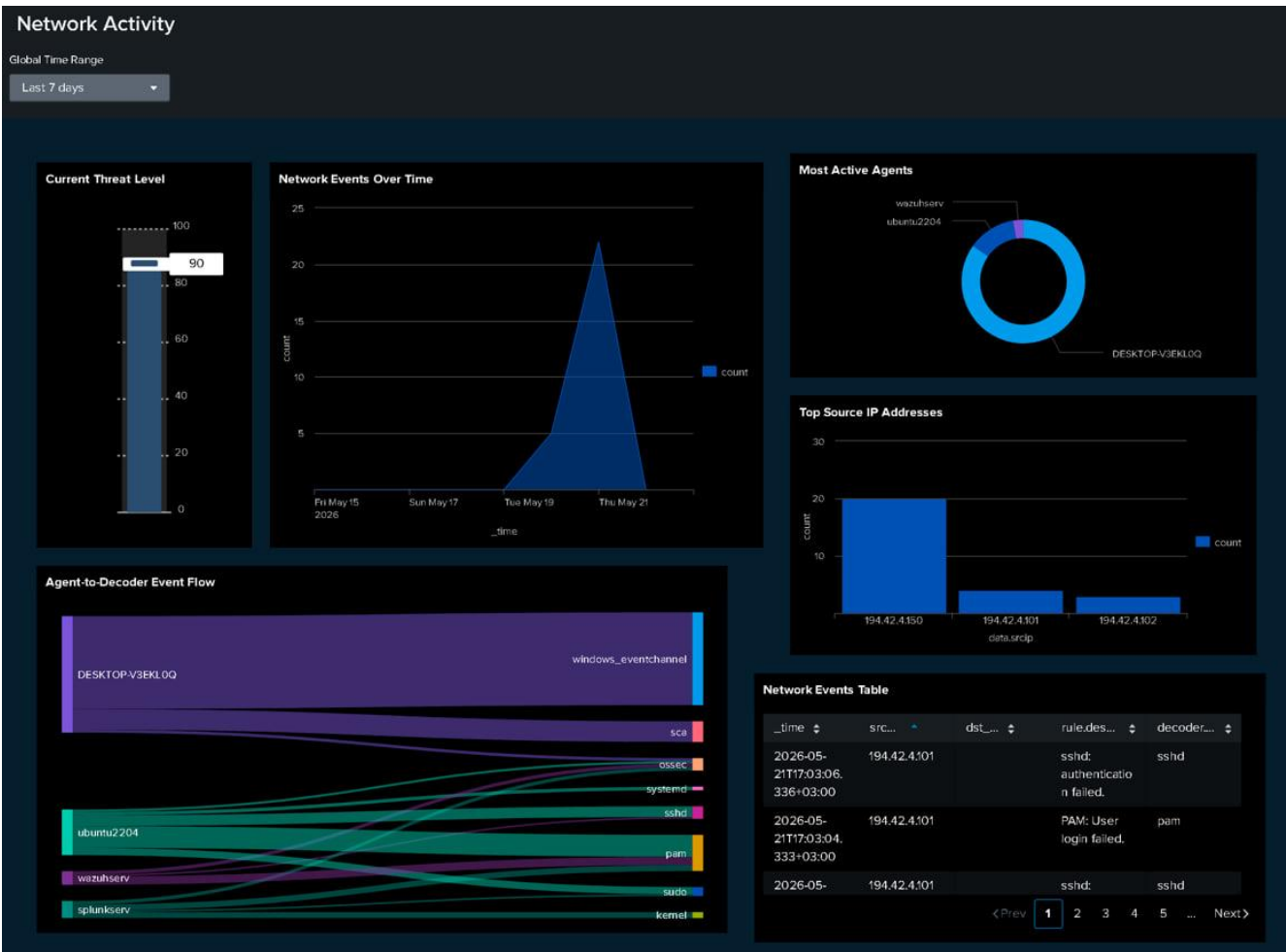


Рисунок 3.14 – Дашборд Network Activity після моделювання інцидентів

На цьому дашборді найбільш помітним є показник Current Threat Level, який після моделювання інцидентів набув високого значення. У реалізованій панелі цей індикатор є умовною оцінкою поточного рівня загрози за шкалою від 0 до 100. Значення формується на основі максимального рівня критичності Wazuh серед мережевих та автентифікаційних подій і перетворюється у категоріальну шкалу для зручності візуального сприйняття.

Графік Network Events Over Time показує сплеск мережевих подій у момент виконання SSH brute-force. Це відповідає очікуваній поведінці, оскільки атака підбору пароля формує серію звернень до SSH-служби цільового Linux-хоста. Елемент Top Source IP Addresses виділяє адресу 194.42.4.150, що дозволяє пов'язати мережеву активність із Kali Linux.

Відображення IP-адрес джерел є важливим для аналізу інцидентів, пов'язаних із мережевою активністю. У випадку SSH brute-force саме поле data.srcip дозволяє відокремити дії Kali Linux від інших подій, що надходять до системи. Завдяки цьому дашборд дає змогу швидко визначити не лише факт підозрілої активності, а й вузол, з якого вона була ініційована.

Візуалізація Most Active Agents показує розподіл мережевих і пов'язаних із ними подій між вузлами. У результатах присутній ubuntu2204, який був ціллю SSH-атаки, а також Windows хост, що формував події через windows_eventchannel. Особливе значення має Agent-to-Decoder Event Flow, оскільки він показує взаємозв'язок між агентами та декодерами. Для Linux хоста відображаються декодери sshd, pam, sudo, systemd та інші, а для Windows хоста – windows_eventchannel. Це підтверджує, що підсистема обробляє події різних типів і з різних операційних систем у єдиному середовищі.

Таблиця Network Events Table дає можливість перейти від загальних мережевих показників до конкретних повідомлень. У ній відображаються події з IP-адресами джерела, описом правила та декодером. Для сценарію SSH brute-force це дозволяє швидко побачити події, пов'язані з 194.42.4.150, і визначити характер мережевої активності.

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				71
Змн.	Арк.	№ докум.	Підпис	Дата		

Останнім було оцінено дашборд Rule & Severity Analysis, призначений для аналізу правил Wazuh, ідентифікаторів правил, груп правил і рівнів критичності.



Рисунок 3.15 – Інформаційна панель Rule & Severity Analysis після моделювання інцидентів

Показник Highest Severity Detected відображає найвищий рівень критичності, зафіксований у вибраному часовому діапазоні. У результаті моделювання інцидентів було отримано події високого рівня, пов'язані з автентифікаційною активністю та повторюваними помилками входу. Це підтверджує, що система не лише реєструє події, а й виділяє серед них більш значущі за рівнем критичності.

Елементи Top Triggered Rules і Rule IDs Frequency дозволяють визначити, які правила Wazuh спрацьовували найчастіше. У результатах присутні правила, пов'язані з SSH-автентифікацією, РАМ-сесіями, системними подіями Windows і службовими повідомленнями. Це дає змогу оцінити не тільки загальну кількість подій, а й те, які саме правила формують основний обсяг повідомлень у системі.

Графік Alerts by Severity Over Time показує, як змінювалися рівні критичності протягом періоду тестування. Сплески на графіку відповідають моментам генерації подій, зокрема SSH brute-force та Windows активності. Діаграма Severity Distribution доповнює цей аналіз і показує загальний розподіл подій за рівнями критичності.

Візуалізація Rule Groups by Severity дозволяє оцінити, які групи правил пов'язані з низькими, середніми або вищими рівнями критичності. Це корисно для визначення категорій подій, що найбільше впливають на загальну картину безпеки. Таблиця Critical Alerts Table дає змогу переглянути конкретні повідомлення з підвищеним рівнем критичності та перейти від зведеного аналізу до окремих подій.

Отримані результати показують, що створені дашборди доповнюють один одного. Security Overview забезпечує загальну оцінку стану підсистеми, Authentication деталізує події входу та спроби автентифікації, Network Activity дозволяє аналізувати джерела мережевої активності, а Rule & Severity Analysis розкриває структуру спрацювань правил Wazuh і розподіл подій за критичністю. У сукупності ці панелі забезпечують перехід від загального огляду до деталізованого аналізу подій безпеки.

Висновки до розділу

У третьому розділі було досліджено роботу реалізованої підсистеми аналізу подій безпеки під час моделювання інцидентів у гетерогенній мережі. Для цього було сформовано декілька сценаріїв активності, що охоплюють спроби підбору пароля до SSH-сервісу, адміністративні дії на Linux-хості, а також події автентифікації та системної активності Windows-хоста.

У процесі моделювання SSH brute-force було встановлено, що Wazuh коректно фіксує події невдалої автентифікації, визначає IP-адресу джерела, цільового користувача, декодер, опис правила та рівень критичності. Після передавання до Splunk ці події стали доступними для пошуку, фільтрації, агрегації та подальшого аналізу за допомогою SPL-запитів.

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				73
Змн.	Арк.	№ докум.	Підпис	Дата		

Під час аналізу адміністративної активності Linux-хоста було підтверджено можливість фіксації локальних дій користувача, зокрема виконання команд із підвищеними привілеями, відкриття та закриття РАМ-сесій, а також створення й видалення тестового користувача. Це показало, що підсистема може використовуватися не лише для аналізу мережесих спроб доступу, а й для контролю змін усередині операційної системи та моніторингу адміністративної активності.

Окремо було перевірено обробку подій Windows-хоста. У Splunk були відображені події успішної та невдалої автентифікації користувача, а також системні події, пов'язані зі зміною стану служб. Це підтвердило можливість централізованого аналізу подій із різних операційних систем у межах єдиного індексу wazuh-alerts.

Оцінювання інформаційних панелей показало, що створені дашборди коректно відображають результати змодельованих інцидентів. Security Overview забезпечує загальний огляд стану підсистеми, Authentication деталізує події входу та невдалі спроби автентифікації, Network Activity дозволяє визначати джерела мережевої активності, а Rule & Severity Analysis відображає спрацювання правил Wazuh і розподіл подій за рівнями критичності. Це підтвердило можливість використання Splunk для централізованої візуалізації та аналізу подій безпеки в гетерогенному середовищі.

Отримані результати тестування підтвердили працездатність реалізованої підсистеми. Вона забезпечує повний цикл обробки подій безпеки, який включає збір, декодування, первинну обробку, передавання, індексацію, пошук, агрегацію та візуалізацію подій із вузлів гетерогенної мережі. Отримані результати свідчать, що підсистема може використовуватися для моніторингу подій безпеки, аналізу інцидентів автентифікації, контролю адміністративної активності, оцінювання рівнів критичності повідомлень та подальшого розширення джерел даних у межах централізованої системи моніторингу.

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				74
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

У кваліфікаційній роботі було виконано проєктування, реалізацію та дослідження роботи підсистеми аналізу подій безпеки гетерогенної мережі з використанням Splunk і Wazuh. Поставленої мети було досягнуто шляхом послідовного виконання теоретичного аналізу, проєктування мережевої структури, розгортання компонентів підсистеми, реалізації механізмів збору й передавання подій, створення інформаційних панелей та перевірки роботи підсистеми під час моделювання інцидентів безпеки.

Було досліджено особливості моніторингу та аналізу подій безпеки в гетерогенних мережах. Встановлено, що використання різних операційних систем, сервісів і форматів журналів подій ускладнює аналіз інцидентів безпеки та потребує застосування централізованого підходу до збору, обробки й візуалізації даних. Також було розглянуто роль SIEM-систем у забезпеченні моніторингу безпеки та своєчасного виявлення підозрілої активності.

Було проаналізовано сучасні SIEM-платформи та засоби моніторингу безпеки, зокрема IBM QRadar, ArcSight, Elastic Security, Graylog, Splunk Enterprise Security та Wazuh. За результатами аналізу визначено, що Splunk Enterprise доцільно використовувати як платформу для індексації, пошуку, агрегації, кореляції та візуалізації подій, а Wazuh – як засіб моніторингу кінцевих вузлів, первинної обробки журналів, застосування правил і формування повідомлень безпеки. Поєднання цих засобів дозволило побудувати підсистему, придатну для роботи з подіями різних операційних систем у межах єдиного централізованого середовища аналізу.

Було спроєктовано структуру гетерогенної мережі, до складу якої увійшли сервер Wazuh, сервер Splunk Enterprise, Windows-хост, Linux-хост і BSD-шлюз на базі pfSense. Визначено адресацію вузлів, їхнє функціональне призначення та роль у загальній архітектурі підсистеми. Така структура дозволила змоделювати роботу системи в умовах мережі з різними операційними системами та різними джерелами подій безпеки.

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				75
Змн.	Арк.	№ докум.	Підпис	Дата		

Було розгорнуто та налаштовано основні компоненти підсистеми: сервер Wazuh, агенти моніторингу на кінцевих вузлах, сервер Splunk Enterprise та Splunk Universal Forwarder. На стороні Wazuh було забезпечено збір, декодування та первинну обробку подій, а на стороні Splunk – приймання, індексацію, пошук, кореляцію та подальший аналіз повідомлень безпеки. Для передавання подій між Wazuh і Splunk було налаштовано моніторинг файлу alerts.json та передавання даних до окремого індексу wazuh-alerts.

Було реалізовано механізм обробки подій, за якого журнали з Windows- та Linux-хостів надходять до Wazuh Manager, проходять декодування, зіставлення з правилами та формуються у вигляді структурованих JSON-повідомлень. Після цього події передаються до Splunk, де стають доступними для SPL-запитів, фільтрації, групування, агрегації та візуалізації. Було розглянуто основні поля подій, зокрема agent.name, rule.description, rule.level, rule.id, decoder.name, data.srcip, data.dstuser та поля Windows Event Log.

Було створено набір інформаційних панелей у Splunk для моніторингу та аналізу подій безпеки. Дашборд Security Overview забезпечує загальний огляд стану підсистеми, Authentication використовується для аналізу подій входу та невдалих спроб автентифікації, Network Activity дозволяє оцінювати джерела мережевої активності, а Rule & Severity Analysis призначений для аналізу правил Wazuh і рівнів критичності подій. Такий поділ забезпечив багаторівневий підхід до моніторингу: від загальної оцінки стану системи до детального аналізу окремих категорій подій.

Було змодельовано інциденти безпеки та перевірено роботу реалізованої підсистеми. Під час моделювання SSH brute-force із використанням Kali Linux було підтверджено фіксацію невдалих спроб автентифікації, визначення IP-адреси джерела, цільового користувача, декодера, опису правила та рівня критичності. Під час аналізу адміністративної активності Linux-хоста було зафіксовано виконання команд із підвищеними привілеями, відкриття та закриття РАМ-сесій, а також створення й видалення тестового користувача. Окремо було перевірено обробку подій Windows-хоста, зокрема подій автентифікації та системної активності.

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				76
Змн.	Арк.	№ докум.	Підпис	Дата		

За результатами тестування встановлено, що реалізована підсистема забезпечує повний цикл централізованої обробки подій безпеки, який включає збір, декодування, первинну нормалізацію, передавання, індексацію, пошук, кореляцію та візуалізацію подій із вузлів гетерогенної мережі. Події з різних операційних систем успішно надходять до єдиного індексу Splunk, зберігають необхідні структуровані поля та можуть використовуватися для аналізу інцидентів, контролю адміністративної активності, оцінювання рівнів критичності й побудови інформаційних панелей. Результати тестування підтвердили працездатність реалізованої підсистеми в умовах гетерогенного мережевого середовища та коректну взаємодію між компонентами Wazuh і Splunk.

Отже, поставлені завдання кваліфікаційної роботи виконано в повному обсязі. Розроблена підсистема аналізу подій безпеки гетерогенної мережі з використанням Splunk і Wazuh може бути використана як основа для централізованого моніторингу подій безпеки, подальшого розширення кількості джерел даних, удосконалення правил аналізу та інтеграції з додатковими засобами виявлення інцидентів.

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				77
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Verizon. 2025 Data Breach Investigations Report. URL:
<https://www.verizon.com/business/resources/T16f/reports/2025-dbir-data-breach-investigations-report.pdf>
2. Paganini P. Reading the ENISA Threat Landscape 2025 report. Security Affairs. 2025. URL: [Reading the ENISA Threat Landscape 2025 report](#)
3. National Institute of Standards and Technology. Cybersecurity Framework. URL: [Cybersecurity Framework | NIST](#)
4. Загальний регламент про захист даних (GDPR). GDPR-Text.com. URL:
<https://gdpr-text.com/uk/>
5. ManageEngine. NIST CSF Detect Function. URL:
<https://www.manageengine.com/log-management/compliance/nist-csf-detect-function.html>
6. Microsoft. Що таке SIEM? URL: <https://www.microsoft.com/uk-ua/security/business/security-101/what-is-siem>
7. IBM. What is SIEM? URL: <https://www.ibm.com/think/topics/siem>
8. IBM. IBM QRadar. URL: <https://www.ibm.com/products/qradar>
9. OpenText. Security Log Analytics. URL:
<https://www.opentext.com/products/security-log-analytics>
10. Elastic. Elastic Stack Security. URL: <https://www.elastic.co/elastic-stack/security>
11. Graylog. Graylog. URL: <https://graylog.org/>
12. Splunk. Splunk Enterprise Security. URL:
https://www.splunk.com/en_us/products/enterprise-security.html
13. Wazuh. Wazuh. URL: <https://wazuh.com/>
14. The FreeBSD Project. FreeBSD Features. URL:
<https://www.freebsd.org/features/>
15. Wazuh. Wazuh Documentation. URL:
<https://documentation.wazuh.com/current/index.html>

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				78
Змн.	Арк.	№ докум.	Підпис	Дата		

16. Wazuh. Wazuh Agent Documentation. URL:
<https://documentation.wazuh.com/current/user-manual/agent/index.html>
17. Splunk. Splunk Documentation. URL:
<https://docs.splunk.com/Documentation/Splunk>
18. Splunk. indexes.conf file reference. URL: <https://help.splunk.com/en/splunk-enterprise/administer/admin-manual/9.4/configuration-file-reference/9.4.0-configuration-file-reference/indexes.conf>
19. Splunk. props.conf file reference. URL: <https://help.splunk.com/en/data-management/splunk-enterprise-admin-manual/10.2/configuration-file-reference/10.2.0-configuration-file-reference/props.conf>
20. Splunk. About forwarding and receiving data. URL:
<https://help.splunk.com/en/splunk-enterprise/forward-and-process-data/forwarding-and-receiving-data/10.4/introduction-to-forwarding/about-forwarding-and-receiving>
21. Splunk. outputs.conf file reference. URL: <https://help.splunk.com/en/splunk-enterprise/administer/admin-manual/10.4/configuration-file-reference/10.4.0-configuration-file-reference/outputs.conf>
22. Splunk. inputs.conf file reference. URL: <https://help.splunk.com/en/splunk-enterprise/administer/admin-manual/9.3/configuration-file-reference/9.3.0-configuration-file-reference/inputs.conf>

ДОДАТКИ

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				80
Змн.	Арк.	№ докум.	Підпис	Дата		

Схема гетерогенної мережі

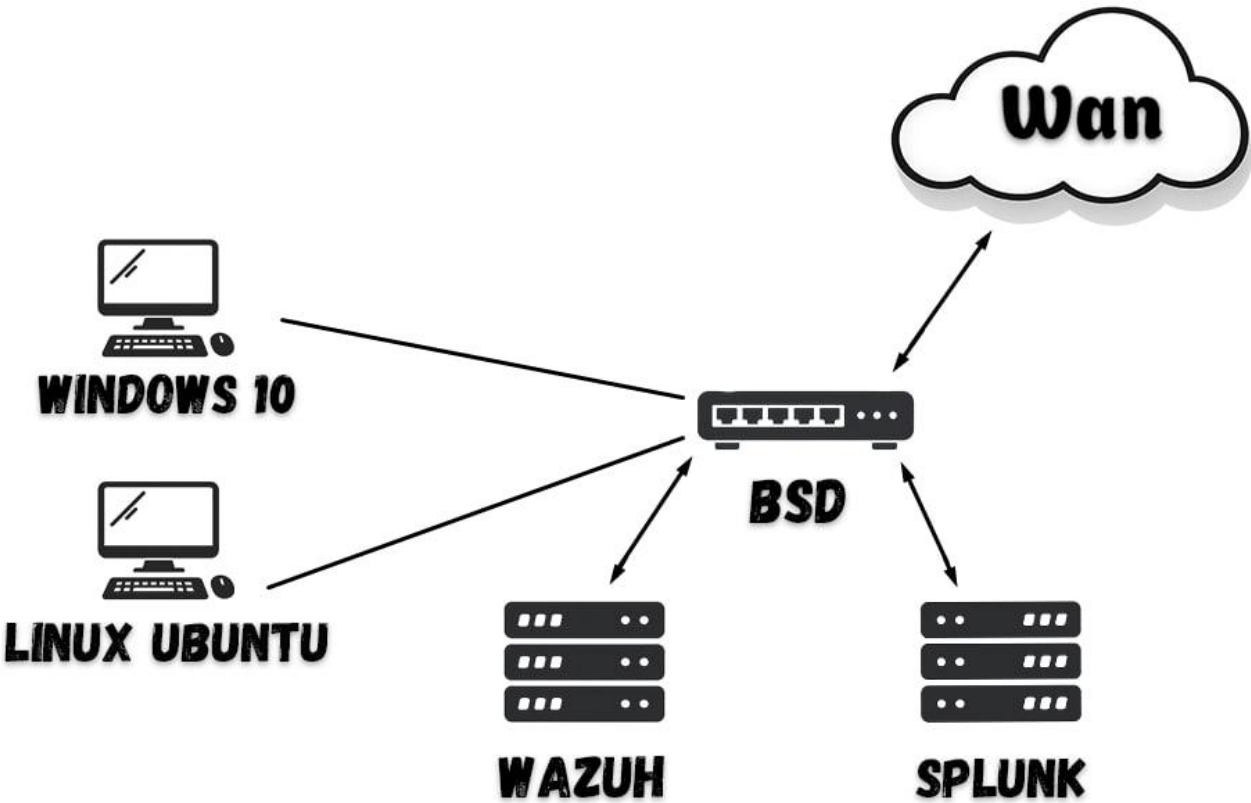


Рисунок А.1 – Загальна структура мережі

Конфігураційні файли Splunk і Splunk Universal Forwarder

Файл Б.1 – inputs.conf (Splunk Enterprise)

[splunktcp://9997]

disabled = 0

Файл Б.2 – indexes.conf (Splunk Enterprise)

[wazuh-alerts]

homePath = /opt/splunk/var/lib/splunk/wazuh-alerts/db

coldPath = /opt/splunk/var/lib/splunk/wazuh-alerts/colddb

thawedPath = /opt/splunk/var/lib/splunk/wazuh-alerts/thaweddb

Файл Б.3 – props.conf (Splunk Enterprise)

[wazuh-alerts]

INDEXED_EXTRACTIONS = JSON

KV_MODE = none

NO_BINARY_CHECK = true

category = Application

pulldown_type = true

Файл Б.4 – outputs.conf (Splunk Universal Forwarder)

[tcpout]

defaultGroup = default-autolb-group

[tcpout:default-autolb-group]

server = 194.42.4.20:9997

[tcpout-server://194.42.4.20:9997]

Файл Б.5 – inputs.conf (Splunk Universal Forwarder)

[monitor:///var/ossec/logs/alerts/alerts.json]

disabled = 0

index = wazuh-alerts

sourcetype = wazuh-alerts

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		82

SPL-запити для інформаційних панелей Splunk

Запит В.1 – Total Alerts (Security Overview)

```
index=wazuh-alerts sourcetype=wazuh-alerts
| stats count
```

Запит В.2 – Critical Alerts (Security Overview)

```
index=wazuh-alerts sourcetype=wazuh-alerts
| spath
| search rule.level>=10
| stats count
```

Запит В.3 – Failed Logins (Security Overview)

```
index=wazuh-alerts sourcetype=wazuh-alerts
| spath
| eval desc=lower('rule.description')
| eval event_id=tostring('data.win.system.eventID')
| eval src=coalesce('data.srcip','data.win.eventdata.ipAddress','')
| eval user=coalesce('data.dstuser','data.srcuser','data.user','data.win.eventdata.targetUserName','')
| eval failed=if(
  like(desc,"%authentication failed%")
  OR like(desc,"%login failed%")
  OR like(desc,"%logon failure%")
  OR like(desc,"%bad password%")
  OR like(desc,"%missed the password%")
  OR event_id="4625",
  1, 0
)
| search failed=1 src!="127.0.0.1"
| bin _time span=30s
| stats count by _time agent.name src user
| stats count as failed_logins
```

Запит В.4 – Active Agents (Security Overview)

```
index=wazuh-alerts sourcetype=wazuh-alerts
| spath
| stats dc(agent.name) as active_agents
```

Запит В.5 – Alerts Over Time (Security Overview)

```
index=wazuh-alerts sourcetype=wazuh-alerts
```

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				83
Змн.	Арк.	№ докум.	Підпис	Дата		

| timechart count

Запит В.6 – Alerts by Severity (Security Overview)

index=wazuh-alerts sourcetype=wazuh-alerts

| spath

| stats count by rule.level

Запит В.7 – Top Agents (Security Overview)

index=wazuh-alerts sourcetype=wazuh-alerts

| spath

| stats count by agent.name

| sort - count

Запит В.8 – Recent Alerts (Security Overview)

index=wazuh-alerts sourcetype=wazuh-alerts

| spath

| table _time agent.name rule.level rule.description

| sort - _time

Запит В.9 – Current Threat Level (Network Activity)

index=wazuh-alerts sourcetype=wazuh-alerts

| spath

| search data.srcip=* OR decoder.name=sshd OR decoder.name=pam

| stats max(rule.level) as max_level

| eval threat_level=case(

max_level>=10, 90,

max_level>=7, 70,

max_level>=5, 50,

max_level>=3, 30,

true(), 10

)

| table threat_level

Запит В.10 – Network Events Over Time (Network Activity)

index=wazuh-alerts sourcetype=wazuh-alerts

| spath

| search data.srcip=* OR data.dstip=*

| timechart count

Запит В.11 – Most Active Agents (Network Activity)

index=wazuh-alerts sourcetype=wazuh-alerts

| spath

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				84
Змн.	Арк.	№ докум.	Підпис	Дата		

```
| search data.srcip=* OR data.dstip=* OR decoder.name=sshd OR decoder.name=windows_eventchannel
| stats count by agent.name
| sort - count
```

Запит В.12 – Top Source IP Addresses (Network Activity)

```
index=wazuh-alerts sourcetype=wazuh-alerts
| spath
| search data.srcip=*
| stats count by data.srcip
| sort - count
| head 10
```

Запит В.13 – Agent-to-Decoder Event Flow (Network Activity)

```
index=wazuh-alerts sourcetype=wazuh-alerts
| spath
| search decoder.name=*
| stats count by agent.name decoder.name
| sort - count
| head 15
| rename agent.name as source
| rename decoder.name as target
```

Запит В.14 – Network Events Table (Network Activity)

```
index=wazuh-alerts sourcetype=wazuh-alerts
| spath
| eval src_ip=coalesce('data.srcip', '-')
| eval dst_ip=coalesce('data.dstip', '-')
| table _time src_ip dst_ip rule.description decoder.name
| sort - _time
```

Запит В.15 – Unique Source IPs (Authentication Monitoring)

```
index=wazuh-alerts
| spath
| search data.srcip=*
| stats dc(data.srcip) as unique_source_ips
```

Запит В.16 – SSH Events Count (Authentication Monitoring)

```
index=wazuh-alerts
| spath
| search decoder.name=sshd
| stats count
```

Запит В.17 – Authentication Failure Rate (Authentication Monitoring)

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				85
Змн.	Арк.	№ докум.	Підпис	Дата		

```

index=wazuh-alerts sourcetype=wazuh-alerts
| spath
| eval desc=lower('rule.description')
| eval event_id=tostring('data.win.system.eventID')
| eval src=coalesce('data.srcip','data.win.eventdata.ipAddress','-')
| eval user=coalesce('data.dstuser','data.srcuser','data.user','data.win.eventdata.targetUserName','-')
| eval failed=if(
    like(desc,"%authentication failed%")
    OR like(desc,"%login failed%")
    OR like(desc,"%logon failure%")
    OR like(desc,"%bad password%")
    OR like(desc,"%missed the password%")
    OR event_id="4625",
    1, 0
)
| search failed=1 src!="127.0.0.1"
| bin _time span=30s
| stats count by _time agent.name src user
| stats count as failure_rate

```

Запит В.18 – Failed Authentication Attempts (Authentication Monitoring)

```

index=wazuh-alerts sourcetype=wazuh-alerts
| spath
| search rule.description="*failed*" OR rule.description="*authentication failed*"
| timechart count

```

Запит В.19 – Sudo Activity (Authentication Monitoring)

```

index=wazuh-alerts sourcetype=wazuh-alerts
| spath
| search rule.description="*sudo*"
| timechart count

```

Запит В.20 – Top Target Users (Authentication Monitoring)

```

index=wazuh-alerts sourcetype=wazuh-alerts
| spath
| eval user=coalesce('data.dstuser', 'data.srcuser', '-')
| stats count by user
| sort - count
| head 10

```

Запит В.21 – Top Source IPs (Authentication Monitoring)

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				
Змн.	Арк.	№ докум.	Підпис	Дата		86

```

index=wazuh-alerts sourcetype=wazuh-alerts
| spath
| search data.srcip=*
| stats count by data.srcip
| sort - count
| head 10

```

Запит B.22 – Failed Login Events Table (Authentication Monitoring)

```

index=wazuh-alerts sourcetype=wazuh-alerts
| spath
| search rule.description="*failed*"
| eval src_ip=coalesce('data.srcip', '-')
| eval user=coalesce('data.dstuser', 'data.srcuser', '-')
| table _time src_ip user rule.description decoder.name
| sort - _time

```

Запит B.23 – Authentication Events Over Time (Authentication Monitoring)

```

index=wazuh-alerts sourcetype=wazuh-alerts
| spath
| eval desc=lower('rule.description')
| eval auth_type=case(
  like(desc,"%failed%") OR like(desc,"%failure%"), "Failed",
  like(desc,"%successful%") OR like(desc,"%accepted%") OR like(desc,"%opened%"), "Successful",
  like(desc,"%sudo%"), "sudo",
  like(desc,"%login%") OR like(desc,"%pam%") OR like(desc,"%sshd%"), "Other auth",
  1=1, "Other"
)
| search auth_type!="Other"
| timechart count by auth_type

```

Запит B.24 – Highest Severity Detected (Rule & Severity Analysis)

```

index=wazuh-alerts
| spath
| stats max(rule.level) as max_severity

```

Запит B.25 – Unique Rule IDs (Rule & Severity Analysis)

```

index=wazuh-alerts
| spath
| stats dc(rule.id) as unique_rules

```

Запит B.26 – Most Common Severity Level (Rule & Severity Analysis)

```

index=wazuh-alerts

```

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				87
Змн.	Арк.	№ докум.	Підпис	Дата		

```
| spath
| stats count by rule.level
| sort - count
| head 1
| fields rule.level
```

Запит В.27 – Total Rule Groups (Rule & Severity Analysis)

```
index=wazuh-alerts
| spath path=rule.groups {} output=rule_group
| mvexpand rule_group
| stats dc(rule_group) as total_groups
```

Запит В.28 – Top Triggered Rules (Rule & Severity Analysis)

```
index=wazuh-alerts sourcetype=wazuh-alerts
| spath
| stats count by rule.description
| sort - count
| head 10
```

Запит В.29 – Severity Distribution (Rule & Severity Analysis)

```
index=wazuh-alerts sourcetype=wazuh-alerts
| spath
| stats count by rule.level
| sort rule.level
```

Запит В.30 – Alerts by Severity Over Time (Rule & Severity Analysis)

```
index=wazuh-alerts sourcetype=wazuh-alerts
| spath
| eval severity=if(isnull('rule.level'), "No level", "Level ".tostring('rule.level'))
| where severity!="No level"
| timechart count by severity
```

Запит В.31 – Rule IDs Frequency (Rule & Severity Analysis)

```
index=wazuh-alerts sourcetype=wazuh-alerts
| spath
| stats count by rule.id
| sort - count
| head 10
```

Запит В.32 – Rule Groups by Severity (Rule & Severity Analysis)

```
index=wazuh-alerts sourcetype=wazuh-alerts
| spath path=rule.groups {} output=rule_group
| spath path=rule.level output=severity_level
```

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				88
Змн.	Арк.	№ докум.	Підпис	Дата		

```

| mvexpand rule_group
| eval severity_num=tonumber(severity_level)
| eval severity=case(
    severity_num<=3, "Low",
    severity_num<=6, "Medium",
    severity_num<=9, "High",
    severity_num>=10, "Critical"
)
| stats count by rule_group severity
| where count >= 10

```

Запит В.33 – Critical Alerts Table (Rule & Severity Analysis)

```

index=wazuh-alerts sourcetype=wazuh-alerts
| spath
| where 'rule.level'>=5
| table _time agent.name rule.level rule.description decoder.name
| sort - _time

```

		Данілевська К.О.			ККІКБ.КР.Б – 125 – 04 – ПЗ	Арк.
		Фальковський І.Г.				89
Змн.	Арк.	№ докум.	Підпис	Дата		

Відповідності джерел подій

Джерело подій	Тип подій	Обробка у Wazuh	Використання у Splunk
Linux auth.log	Події автентифікації Linux, SSH-підключення, невдалі спроби входу, PAM-сесії, використання sudo	Події обробляються відповідними декодерами Wazuh, зокрема sshd, pam та sudo, після чого зіставляються з правилами виявлення	Використовується для аналізу SSH brute-force, невдалих спроб автентифікації, відкриття та закриття сесій, а також адміністративної активності користувачів
Linux системні журнали	Події зміни стану системи, створення та видалення користувачів, службові повідомлення операційної системи	Wazuh Agent передає системні журнали до Wazuh Manager, де вони декодуються та перетворюються на структуровані повідомлення безпеки	Використовується для аналізу змін у системі облікових записів, зокрема створення та видалення тестового користувача
Windows Security Log	Події безпеки Windows, зокрема успішні та невдалі спроби входу користувачів	Події отримуються агентом Wazuh із журналів Windows Event Log та обробляються через механізм windows_eventchannel	Використовується для аналізу подій автентифікації Windows-хоста, визначення користувача, статусу входу та ідентифікатора події
Windows System Log	Системні події Windows, повідомлення служб, зміна стану або параметрів системних компонентів	Події збираються агентом Wazuh із системного журналу Windows та обробляються через windows_eventchannel	Використовується для аналізу системної активності Windows-хоста, зокрема подій, пов'язаних зі службами
Wazuh alerts.json	Сформовані Wazuh повідомлення безпеки після обробки журналів кінцевих вузлів	Файл формується Wazuh Manager після застосування декодерів і правил до подій, отриманих від агентів	Використовується як джерело для передавання подій до Splunk через Splunk Universal Forwarder та подальшої індексації в wazuh-alerts
Sysmon	Події процесів, мережних з'єднань, змін файлів і реєстру	Може оброблятися Wazuh Agent після встановлення Sysmon і налаштування збору відповідного каналу	Може використовуватися для розширеного аналізу активності Windows-хоста